ADSL Modem HM210dp/di
User Guide

Contents page

1 Introduction

Congratulations on becoming the owner of an Ericsson ADSL Modem HM210dp/di. Your LAN (Local Area Network) will now be able to access the Internet using your high-speed ADSL connection. This User Guide describes how to install and set up your HM210dp/di in a Windows environment, and how to customize its configuration to get the most out of your new product.

1.1 Features

The ADSL Modem HM210 comes in two versions: HM210dp and HM210di. Both products offer the same features, but they rely on different types of telephone line in order to provide the ADSL service. **HM210dp** offers ADSL service over POTS (Plain Old Telephone System) lines, while **HM210di** uses ISDN (Integrated Services Digital Network) lines to provide the ADSL service.

The main features of the HM210dp/di are listed below:

- Internal ADSL modem for high-speed Internet access.
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN.
- Network address translation (NAT) and IP filtering functions to provide firewall protection for your computers.
- Network configuration through DHCP.
- Configuration Manager program you access via a web browser.

1.2 Package Contents

Your package should contain all the components listed below. If any component is missing or damaged, please contact the ADSL modem provider.

- ADSL Modem HM210dp/di
- A Power Supply Adapter with connecting cable
- Ethernet cable (straight-through)
- ADSL Line cable
- Quick Installation Guide.

Note:

Your package may also include other materials provided by your ADSL operator.

1.3 System Requirements

In order to use your HM210dp/di, you must have the following:

- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN.

- One or more computers each containing an Ethernet 10Base-T/100Base-T network interface card (NIC).
- An Ethernet hub/switch, if you are connecting the device to more than one computer.
- For system configuration using the built-in Configuration Manager program: a web browser such as Internet Explorer v5.0 or later, or Netscape v5.0 or later.

2 Hardware Description and Connection

2.1 Front Panel and LED Indicators

The front panel of the HM210dp/di contains five control lamps (LEDs) that indicate the status of the modem:

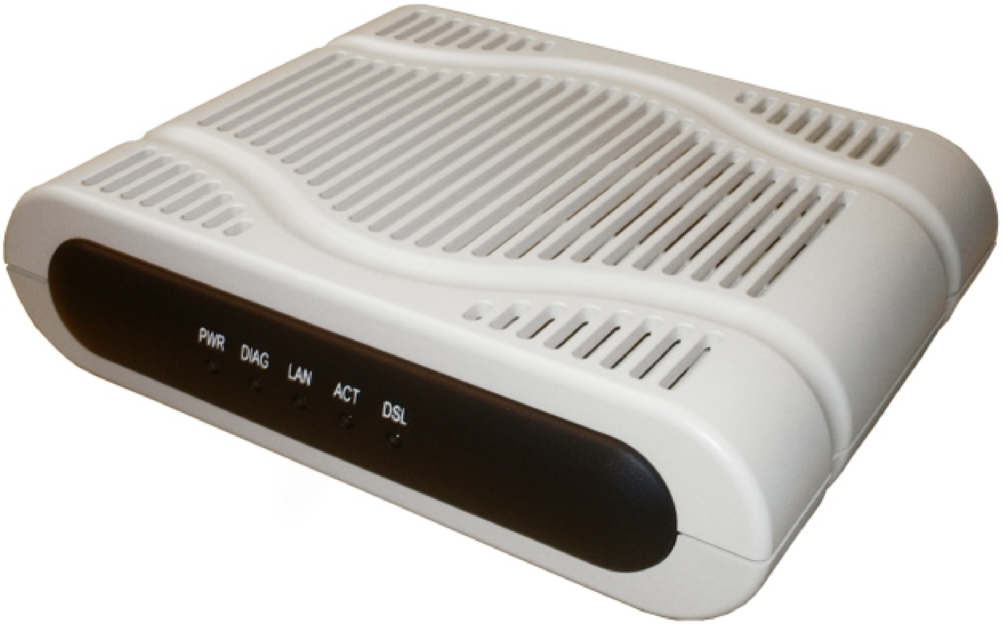


Figure 1: Front Panel of HM210dp/di

Label	Color	Function
PWR	green	ON: Unit is powered on. OFF: Unit is powered off.
DIAG	green	Flashes ON/OFF at boot-up to indicate that the device software is operational.
LAN	green	OFF: No Ethernet link detected. ON: Ethernet link established and active.
ACT	green	Flashes when ADSL data activity occurs. May appear solid when data traffic is heavy.
DSL	green	OFF: No ADSL link detected. ON: ADSL link established and active.

2.2 Back Panel and Connectors

The back panel of the HM210dp/di contains the connectors for the unit's data and power connections as described below:

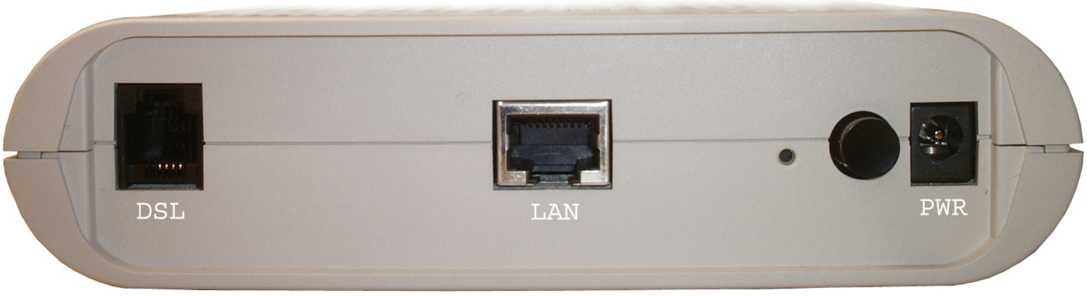


Figure 2: Back Panel of HM210dp/di

Label	Function
DSL	Connects the HM210dp/di to an ADSL outlet (splitter/filter or phone outlet) using the supplied ADSL Line cable.
LAN	Connects the HM210dp/di to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the supplied Ethernet cable.
Reset button (tiny hole)	Used to restore the HM210dp/di to its original factory default settings. To reset the device to factory defaults, you don't need to power off the device. Just push a paper clip into the hole and hold for 3 times before releasing. Then wait for the device to finish boot-up.
Power button	Used to switch the HM210dp/di ON and OFF.
PWR	Power socket for connecting the HM210dp/di to a power outlet by using the supplied power adapter.

2.3 Placement

The HM210dp/di should be placed on a flat surface. Be sure to choose a location that enables you to see the LEDs, is close to a power outlet, ADSL outlet, and the PC.

Note:

Proper ventilation is necessary to prevent the product from over-heating. Do not block or cover the slots and openings on the device, which are intended for ventilation and proper operation.

2.4 Connecting the Hardware

Follow the procedures below to connect related devices. Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the HM210dp/di.

1 **Connect to the ADSL Line**.

Connect one end of the provided **ADSL Line cable** to the port labeled **DSL** on the back panel of the HM210dp/di. Connect the other end to your ADSL service port (splitter/filter or phone outlet).

Note:

Depending on the service type offered by your ISP, an additional splitter may be needed. If this is the case, consult with your ISP for actual connection.

2 **Connect to a PC or hub/switch.**

- **To a single PC** - Attach one end of the provided **Ethernet cable** (straight-through) to the port labeled **LAN** on the HM210dp/di. Connect the other end to your PC's Ethernet port.
- **To a hub/switch** - Attach one end of a "cross-over" Ethernet cable to a hub/switch and the other end to the **LAN** port on the HM210dp/di.
- **To a hub/switch's uplink port**: - Use a "straight-through" cable to connect it to the uplink port and the other end to the **LAN** port on the HM210dp/di.

3 **Attach the power connector**.

Connect the provided **Power cable** to the **PWR** socket on the HM210dp/di. Plug the power supply adapter into a power source (wall outlet or power strip).

4 **Turn on the HM210dp/di and power up your systems**.

Press the **Power** button on the back panel of the HM210dp/di to turn on the device.

Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

3 Local PC Configuration

By default, the HM210dp/di acts as DHCP server that automatically assigns all required Internet settings to your PCs, i.e., the DHCP clients. The predefined IP address and DHCP pool is as below:

LAN Port IP address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP pool	192.168.1.3 - 34

The following instructions assume that your PC meets the following prerequisites:

1 Already is connected to the LAN port on the HM210dp/di through its network interface card (NIC).

2 Has the appropriate Ethernet adapter software.

3 Has the TCP/IP protocol installed. If not, refer to Microsoft documentations to install the TCP/IP protocol.

You need only to configure the PCs to accept the information when it is assigned. Follow the instructions that correspond to the operating system installed on each PC.

3.1 Configuring your PCs as DHCP Clients

3.1.1 In Windows 95, 98 and Me

1 In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.

2 Double-click the **Network** icon.

3 On **Configuration** tab, select the TCP/IP network associated with your network card and then click **Properties**.

4 In the **TCP/IP Properties** dialog box, click the **IP Address** tab.

5 Click the radio button labeled **Obtain an IP address automatically**.

6 Click **OK** twice to confirm and save your changes.

7 You will be prompted to restart Windows. Click **Yes**.

3.1.2 In Windows 2000 and XP

1 In the Windows task bar, click the **Start** button, point to **Settings**, and then click the **Control Panel**.

2 Double-click the **Network and Dial-up Connections** (or **Network Connections** for Windows XP) icon.

3 Right-click the **Local Area Connection** icon, and then select **Properties**.

4 Highlight **Internet protocol (TCP/IP)**, and then click **Properties**.

5. In the **Internet protocol (TCP/IP) Properties** dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
6. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

3.2 Assigning Static IP Information to your PCs

In some cases, you may want to assign static IP information to your PC directly if:

- In **bridge** mode, you have completed initial configuration and you need to use the IP address and default gateway given by your ISP.
- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN.

Before you begin, contact your ISP if you do not already have the following information:

- IP address and subnet mask.
- Default Gateway
- DNS Server

On each PC to which you want to assign static information, follow the instructions for displaying each of the TCP/IP properties (described in the previous section). Instead of enabling dynamic assignment of the IP addresses for the computer, click the radio buttons that enable you to enter the IP address, DNS and default gateway manually.

4 Getting Started with the Configuration Manager

Your HM210dp/di includes a web-based Configuration Manager, which enables you to configure the device settings to meet the needs of your network.

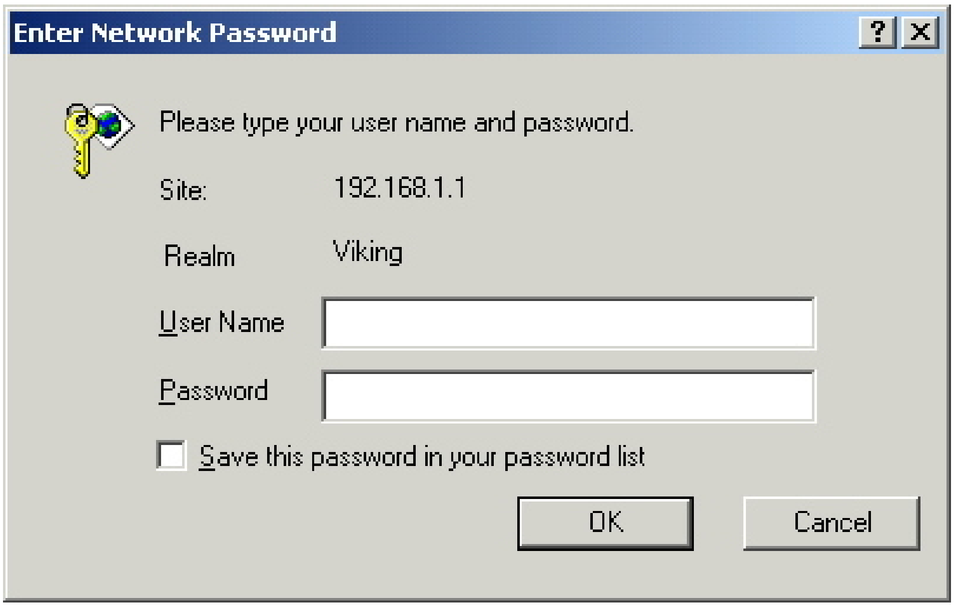
4.1 Accessing the Configuration Manager

You can access the Configuration Manager from any computer connected to the HM210dp/di.

1 At any PC connected to the HM210dp/di, open a web browser, type the following URL in the web address (or location) box, and press <Enter>:

```
http://192.168.1.1
```

2 When the login screen appears, enter your User Name and Password, and then click **OK**.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm Viking

User Name

Password

□ Save this password in your password list

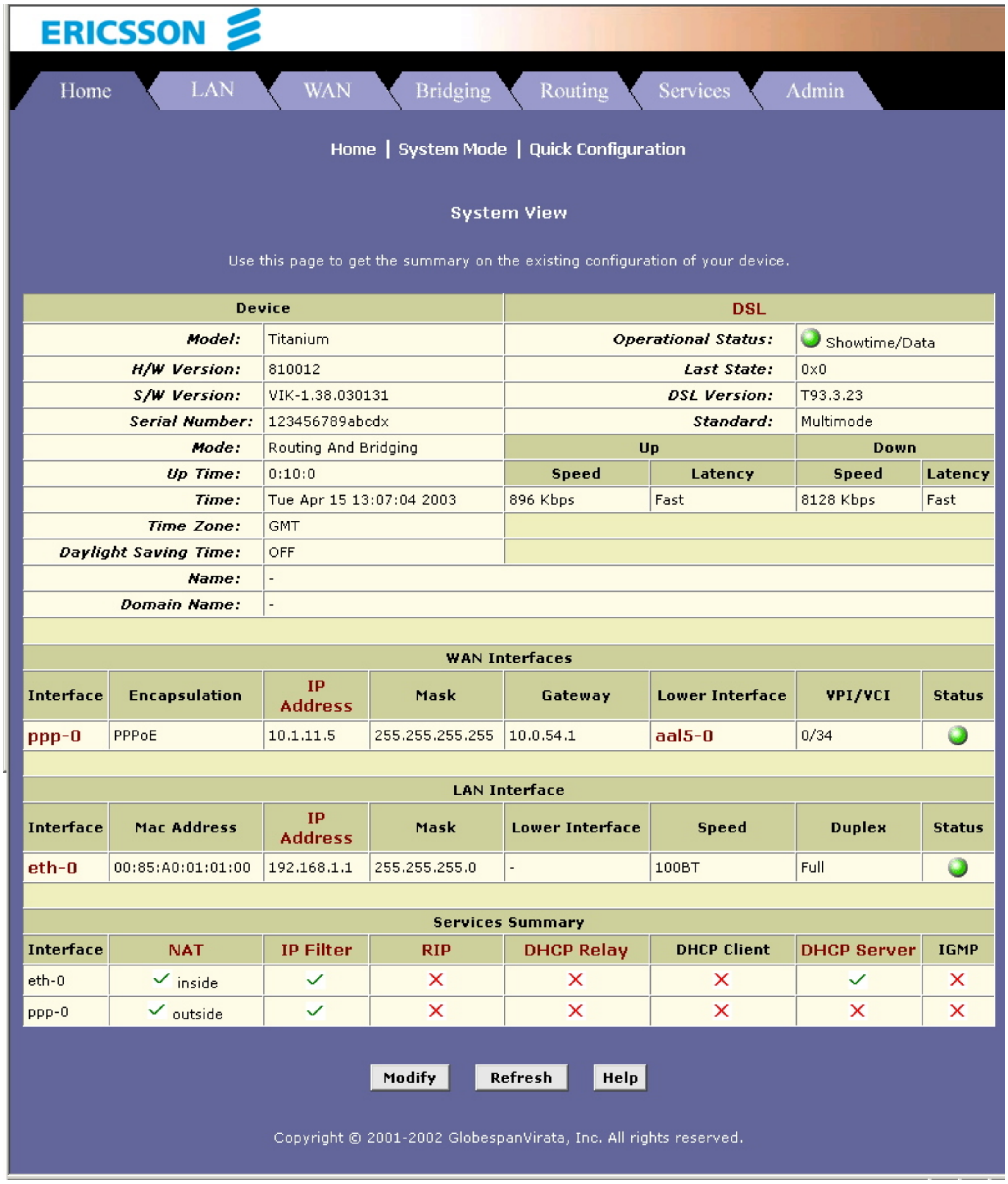
Figure 3: Login window

The first time you launch the Configuration Manager, use these default values:

Default User Name: **root**

Default Password: **root**

After a successful login, the **System View** page appears.



System View

Use this page to get the summary on the existing configuration of your device.

Device	
Model:	Titanium
H/W Version:	810012
S/W Version:	VIK-1.38.030131
Serial Number:	123456789abcdx
Mode:	Routing And Bridging
Up Time:	0:10:0
Time:	Tue Apr 15 13:07:04 2003
Time Zone:	GMT
Daylight Saving Time:	OFF
Name:	-
Domain Name:	-

DSL			
Operational Status:		● Showtime/Data	
Last State:		0x0	
DSL Version:		T93.3.23	
Standard:		Multimode	
Up		**Down**	
Speed	**Latency**	**Speed**	**Latency**
896 Kbps	Fast	8128 Kbps	Fast

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoE	10.1.11.5	255.255.255.255	10.0.54.1	aal5-0	0/34	●

LAN Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	192.168.1.1	255.255.255.0	-	100BT	Full	●

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✓	✗	✗	✗	✓	✗
ppp-0	✓ outside	✓	✗	✗	✗	✗	✗

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 4: System View

The System View table provides a snapshot of your system configuration. You can click on the provided links that enable you to configure each setting (if available). Refer to the appropriate chapters in this document for more information.

4.2 Commonly Used Buttons and Icons

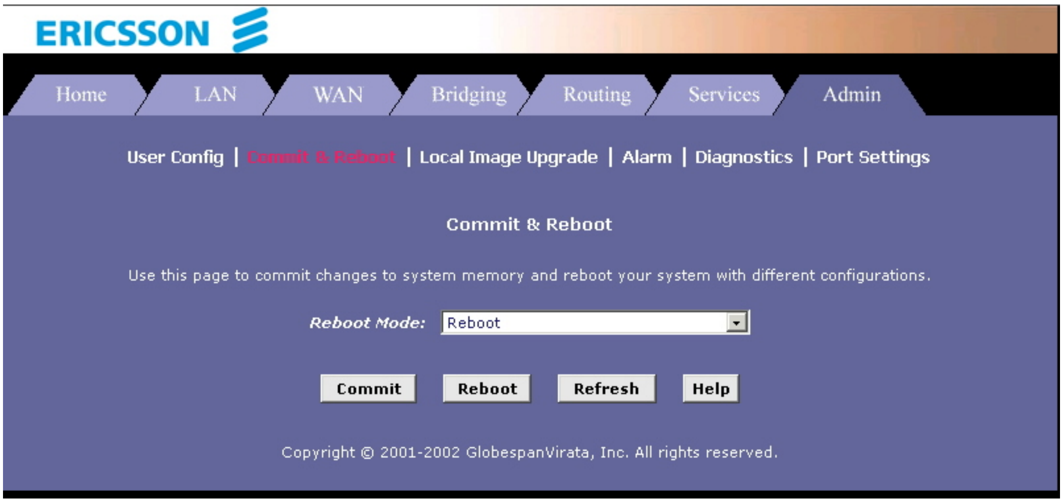
Button / Symbol	Function
Submit	Stores in temporary system memory any changes you have made on the current page.
Refresh	Redisplays the current page with updated statistics.
Clear	When accumulated statistics are displaying, this button resets the statistics to their initial values.
Help	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.
🗑	Delete an entry.
✏	Modify an entry.
🔍	View details for an entry.

4.3 Committing Changes to Permanent Storage

Whenever you change system settings, the changes are initially placed in a temporary storage (called random access memory or RAM). Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

Follow these steps to commit changes to permanent storage.

1 Select **Admin** > **Commit & Reboot**. The **Commit & Reboot** page appears:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Commit
Reboot
Refresh
Help

Commit & Reboot

Use this page to commit changes to system memory and reboot your system with different configurations.

Reboot Mode: Reboot

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 5: Commit & Reboot page

2 Click the **Commit** button. (Disregard the selection in the "Reboot Mode" drop-down list; it does not affect the commit process).

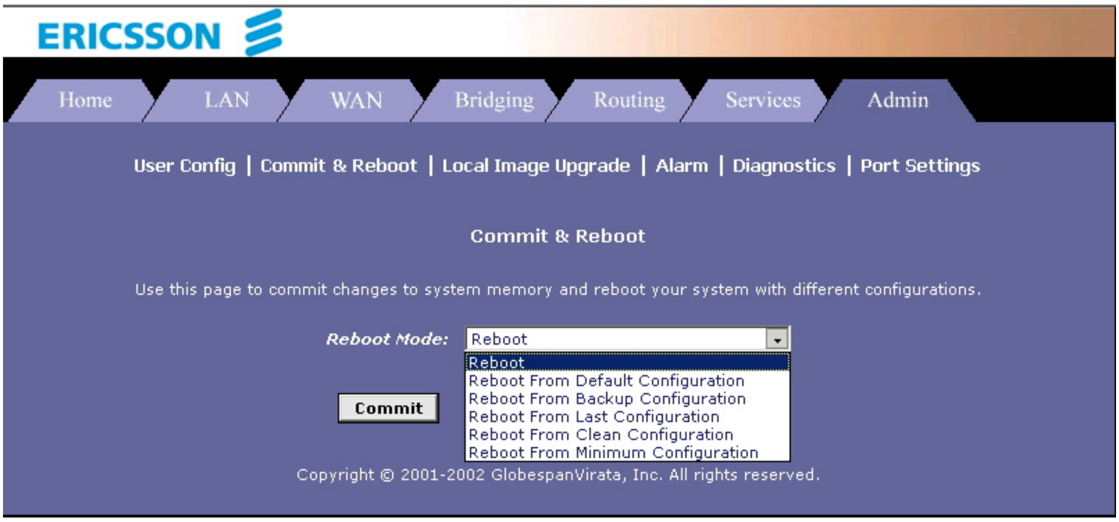
The changes are saved to permanent storage.

Note:

If you change the LAN IP address information, you MUST commit the changes and then reboot the system to activate them. All other changes are activated when you commit them (no reboot is needed).

4.3.1 Rebooting the HM210dp/di using the Configuration Manager

If, after rebooting the device, you find that it does not operate properly with the new configuration, you can reboot using options that reactivate a previous configuration or the factory default configuration.


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Commit
Reboot
Reboot From Default Configuration
Reboot From Backup Configuration
Reboot From Last Configuration
Reboot From Clean Configuration
Reboot From Minimum Configuration

Commit & Reboot

Use this page to commit changes to system memory and reboot your system with different configurations.

Reboot Mode: Reboot

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 6: Reboot Mode page

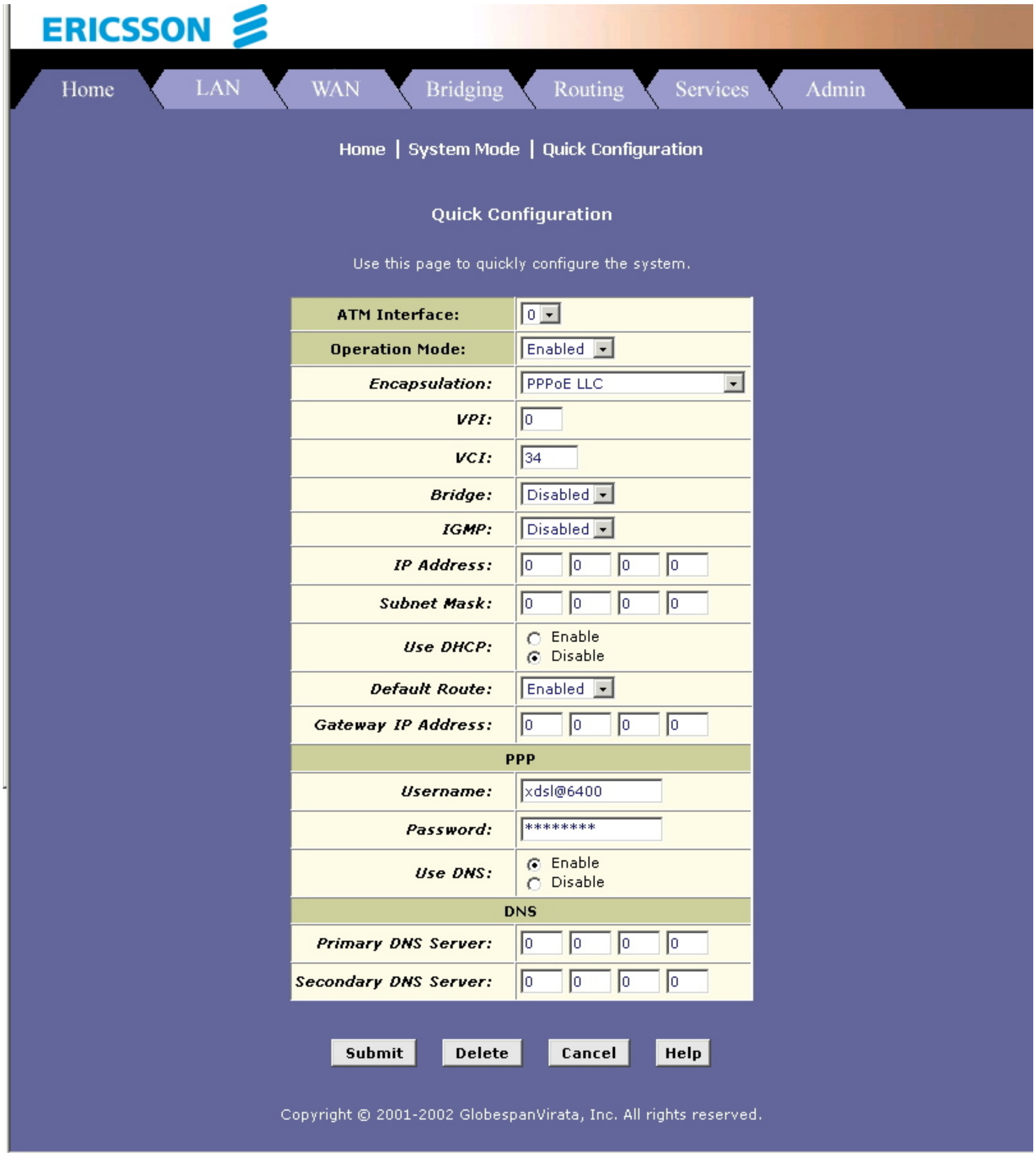
You can select from the following options when rebooting:

Setting	Description
Reboot	Reboots the device to activate your new settings (if any).
Reboot from Default Configuration	Reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.
Reboot from Backup Configuration	Reboots the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot from Last Configuration	Reboots the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Clean Configuration	
Reboot from Minimum Configuration	

4.4 Quick Configuration

The **Quick Configuration** page allows you to quickly configure your HM210dp/di for Internet connection. Your ISP should provide you with necessary information to complete the quick setup.

To quickly configure the system, go to **Home** > **Quick Configuration**. The **Quick Configuration** page appears:



Quick Configuration

Use this page to quickly configure the system.

ATM Interface:	0
Operation Mode:	Enabled
Encapsulation:	PPPoE LLC
VPI:	0
VCI:	34
Bridge:	Disabled
IGMP:	Disabled
IP Address:	0 0 0 0
Subnet Mask:	0 0 0 0
Use DHCP:	○ Enable ● Disable
Default Route:	Enabled
Gateway IP Address:	0 0 0 0
PPP	
Username:	xdsl@6400
Password:	********
Use DNS:	● Enable ○ Disable
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 7: Quick Configuration page

Enter the provided fields as below:

Field	**Description**
ATM Interface	Select the ATM interface you want to use (usually atm-0) for this connection.

Field	Description
Operation Mode	Select **Enabled**. If set to **Disabled**, the device cannot provide Internet connectivity for your network.
Encapsulation	Select the connection type your ISP uses to communicate with your HM210dp/di.
VPI and VCI	Enter the VPI/VCI values given by your ISP.
Bridge	This setting enables or disables bridging between the HM210dp/di and your ISP. Your ISP may also refer to this using "RFC 1483" or "Ethernet over ATM".
IGMP	This setting enables or disables the Internet Group Management Protocol. Contact your ISP whether to enable this setting.
IP Address and Subnet Mask	If your ISP has assigned a public IP address to your LAN, enter the IP address and the associated subnet mask in the boxes provided. Otherwise keep the default 0.0.0.0/0.0.0.0.
Use DHCP	
Default Route	When enabled, the IP address specified above will be used as the default route for your LAN.
Gateway IP Address	Specify the IP address that identifies the ISP server through which your Internet connection will be routed.
Username and Password	If you select PPP as the Encapsulation type, enter the username and password you use to log in to your ISP.
Use DNS	Click **Enable** to turn on the DNS forwarding service, which forwards to your LAN PCs the DNS server addresses that your PPP connection learns from your ISP. This option can only be used when the HM210dp/di acts as a DHCP server for your LAN.
Primary/Secondary DNS Server	You may just keep the default 0.0.0.0. If you enter the Primary and Secondary DNS addresses given by your ISP, these DNS servers will be used in addition to any DNS servers discovered automatically.

After completing the required settings, click the **Submit** button.

Go to **Admin > Commit & Reboot** and click **Commit** to store your changes to permanent memory.

5 Basic Configuration

This chapter provides basic configuration instructions to get your HM210dp/di run and have your network connected to the Internet.

The instructions assume that the HM210dp/di is not predefined with any ATM VC, PPP and IPoA settings. For each connection method, example parameters are given for your better understanding. You should consult with your ISP to determine your connection mode and enter the actual values provided by your ISP.

Note:

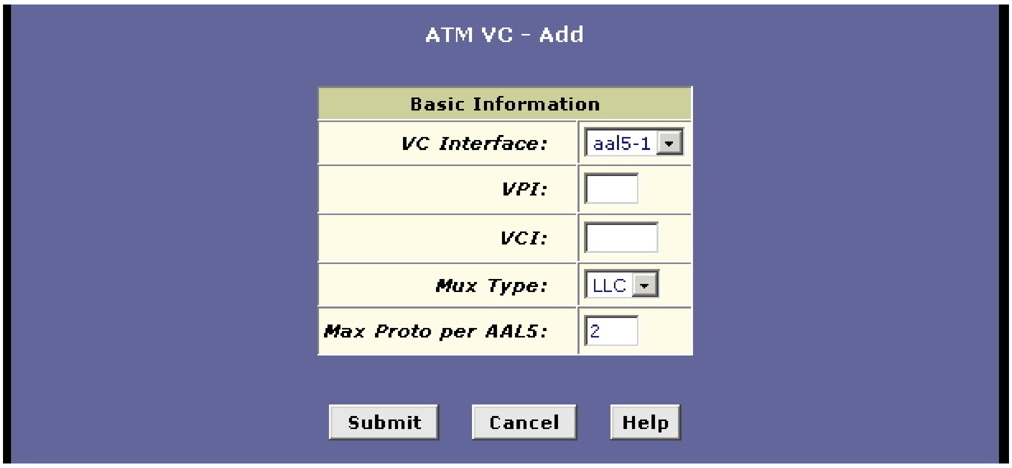
Your HM210dp/di may already be preconfigured with the necessary settings to get your network connected to the Internet. Contact your ISP to determine whether you should change any existing values.

5.1 Bridge Mode

5.1.1 Configuring the HM210dp/di

1 **Creating an ATM VC interface**:

a Select **Bridging** > **ATM VC** > **Add**. The **ATM VC - Add** page appears:



ATM VC - Add

Basic Information	
VC Interface:	aal5-1
VPI:	
VCI:	
Mux Type:	LLC
Max Proto per AAL5:	2

Figure 8: ATM VC - Add

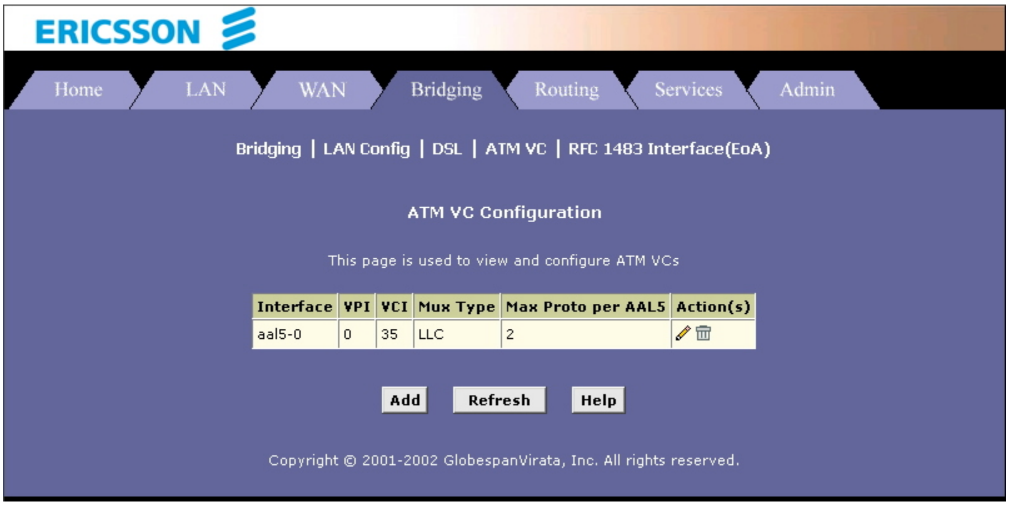
b Enter the provided fields as below:

Field	Description
VC Interface	Select a VC interface from the available interfaces, e.g. **aal5-0** .
VPI and VCI	Enter the VPI/VCI values given by your ISP, e.g. **0/33**
Mux Type	Select **LLC** or **VC** as required by your ISP.
Max Proto per AAL5	Keep the default **2**.

After entering the fields above, click the **Submit** button.

c When the confirmation page appears, click **Close**.

d You will return to the **ATM VC Configuration** table and see the newly added ATM VC entry.


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)

ATM VC Configuration

This page is used to view and configure ATM VCs

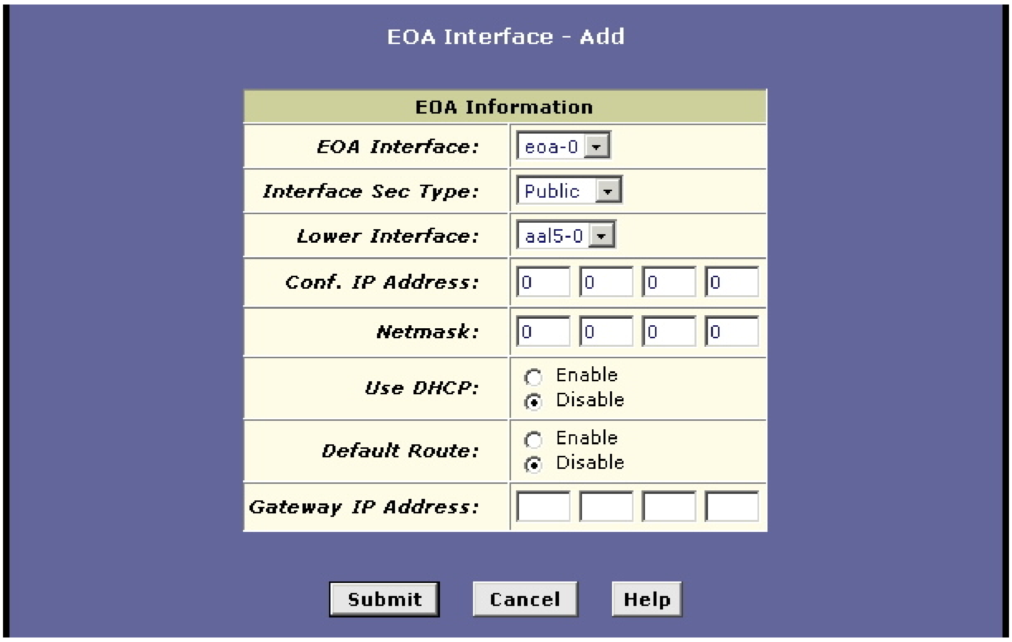
Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	0	35	LLC	2	✎ 🗑

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 9: ATM VC Configuration

2 **Creating an EoA interface**:

a Select **Bridging** > **RFC1483 Interface (EoA)** > **Add** to add a new EoA interface:



EOA Interface - Add

EOA Information

EOA Interface:	eoa-0
Interface Sec Type:	Public
Lower Interface:	aal5-0
Conf. IP Address:	0 . 0 . 0 . 0
Netmask:	0 . 0 . 0 . 0
Use DHCP:	○ Enable ● Disable
Default Route:	○ Enable ● Disable
Gateway IP Address:	

Figure 10: EOA Interface - Add

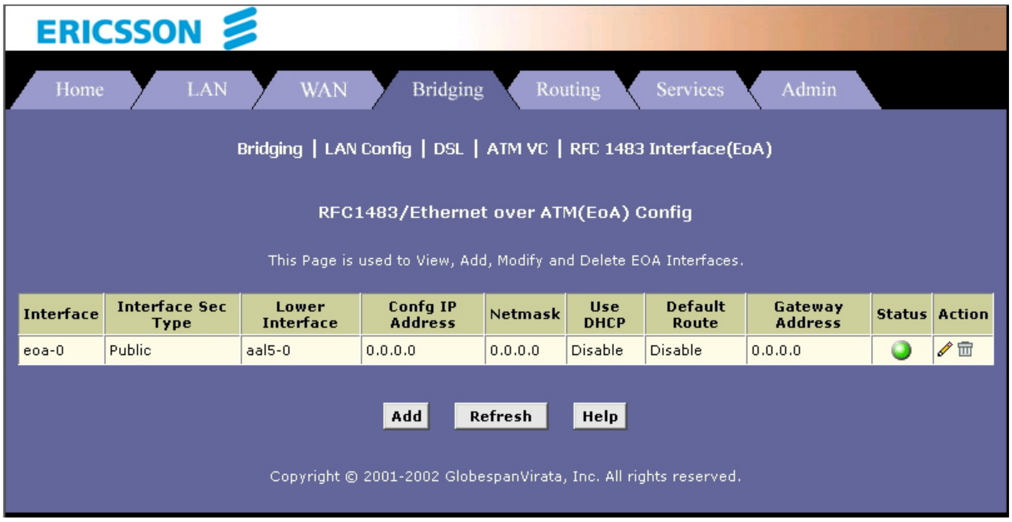
b Enter the provided fields as below:

Field	Description
EOA Interface	Select an EoA interface from the available interfaces, e.g. **eoa-0** .
Interface Sec Type	**Public**
Lower Interface	Select the ATM VC interface you created in Step 1, e.g. **aal5-0** .
Config. IP Address/Net Mask	**0.0.0.0 / 0.0.0.0** To use the HM210dp/di as a bridge, you don't need to set the IP address and subnet mask. Just keep the default.
Use DHCP	**Disable**
Default Route	**Disable**
Gateway IP Address	Leave it empty. You don't need to set the gateway.

After entering the fields above, click the **Submit** button.

c When the confirmation page appears, click **Close**.

d You will return to the **EOA** table and see the newly added EOA entry.


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)
Add
Refresh
Help

RFC1483/Ethernet over ATM(EoA) Config

This Page is used to View, Add, Modify and Delete EOA Interfaces.

Interface	Interface Sec Type	Lower Interface	Confg IP Address	Netmask	Use DHCP	Default Route	Gateway Address	Status	Action
eoa-0	Public	aal5-0	0.0.0.0	0.0.0.0	Disable	Disable	0.0.0.0	●	✎ 🗑

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 11: RFC1483/Ethernet over ATM(EoA) Config

3 **Enable Bridging function**:

a Select **Bridging** > **Bridging** page to display the **Bridge Configuration** page.

b Select **eth-0** from the list and click **Add**.

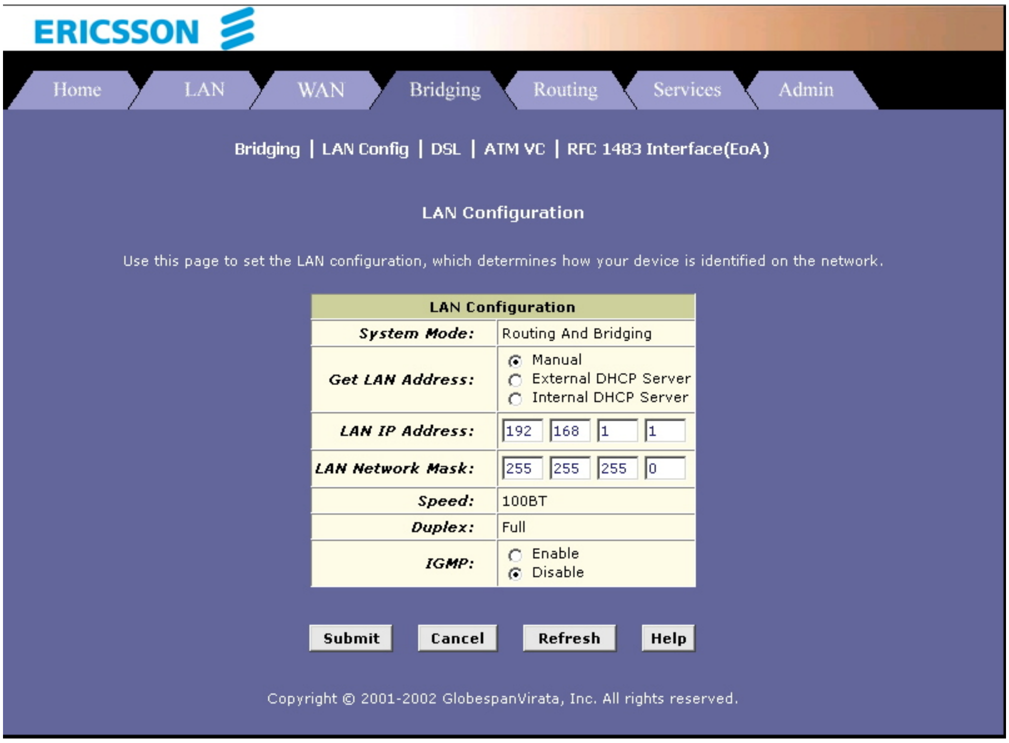
c Select the EOA interface to be used (e.g. **eoa-0**) from the drop-down list, and then click **Add**.

d Set the Bridging item to **Enable** and click **Submit**. A confirmation page appears to confirm your changes.

4 **LAN configuration**:

a Select **Bridging** > **LAN Config**.

b Don't modify the settings; just keep the default as shown in the figure below:



LAN Configuration

Use this page to set the LAN configuration, which determines how your device is identified on the network.

LAN Configuration	
System Mode:	Routing And Bridging
Get LAN Address:	● Manual ○ External DHCP Server ○ Internal DHCP Server
LAN IP Address:	192 168 1 1
LAN Network Mask:	255 255 255 0
Speed:	100BT
Duplex:	Full
IGMP:	○ Enable ● Disable

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

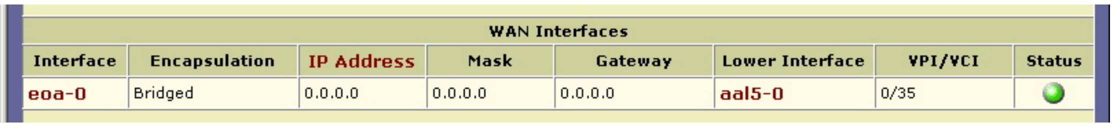
Figure 12: LAN Configuration

5 **Commit your changes**:

Select **Admin** > **Commit & Reboot** and click **Commit** to store your changes to permanent memory.

5.1.2 Check Your Connection Status

Select **Home** > **System Mode**. The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection.



WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
eoa-0	Bridged	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	0/35	●

Figure 13: WAN IF Status

5.1.3 Configuring the PC

- **Option 1: Your PC uses the IP information given by your ISP**.

  If this is the case, configure your PC to use the static IP information given by your ISP, for example:

  IP address: 10.100.16.2

  Subnet mask: 255.255.255.0

  Default gateway: 10.100.16.254

  NOTE! With the configuration above, your PC should be able to access the Internet now but will lose the local connection to the device's LAN port. If you want to configure the HM210dp/di via the Configuration Manager again, you should re-configure the PC to **192.168.1.x** to be in the same subnet of the device's LAN port.

- **Option 2: Your client use PPPoE software to connect to your ISP**.

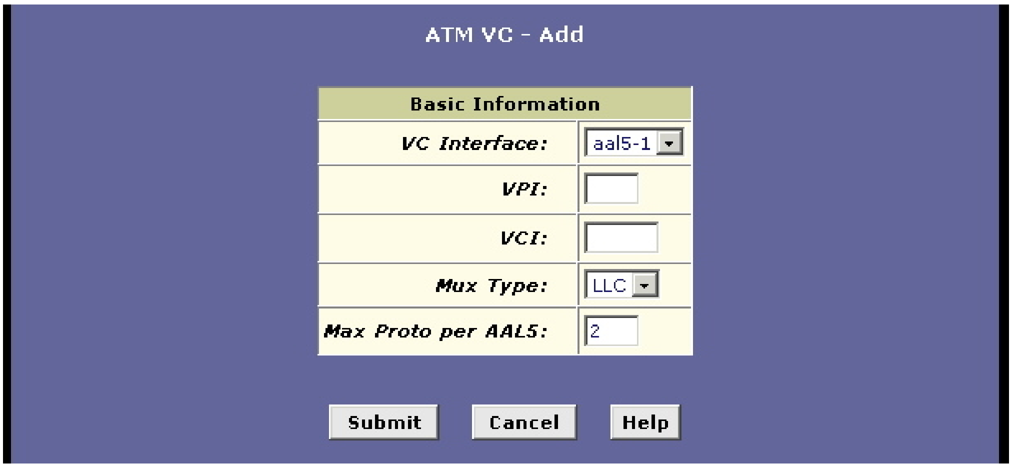
  Just keep your PC's setting as a DHCP client and execute the PPPoE software to make the connection.

5.2 PPP Connection Mode

5.2.1 Configuring the HM210dp/di

1 **Creating an ATM VC interface**:

a Select **Routing** > **ATM VC** > **Add**. The **ATM VC - Add** page appears:



ATM VC - Add

Basic Information

VC Interface: aal5-1

VPI:

VCI:

Mux Type: LLC

Max Proto per AAL5: 2

Figure 14: ATM VC - Add

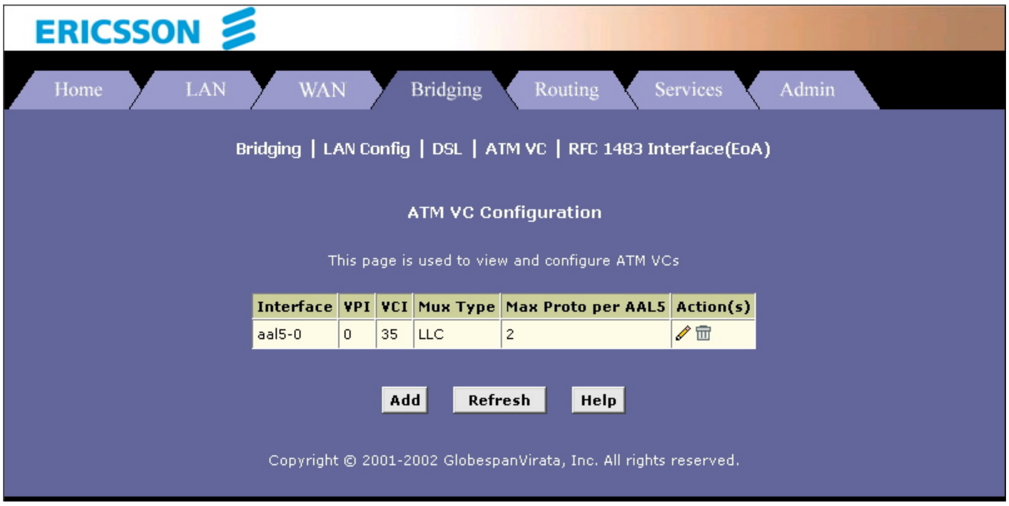
b Enter the provided fields as below:

Field	Description
VC Interface	Select a VC interface from the available interfaces, e.g. **aal5-0** .
VPI and VCI	Enter the VPI/VCI values given by your ISP, e.g. **0/33**
Mux Type	For PPPoE, select **LLC** For PPPoA, select **VC**.
Max Proto per AAL5	Keep the default **2**.

After entering the fields above, click the **Submit** button.

c When the confirmation page appears, click **Close**.

d You will return to the **ATM VC Configuration** table and see the newly added ATM VC entry.


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)

ATM VC Configuration

This page is used to view and configure ATM VCs

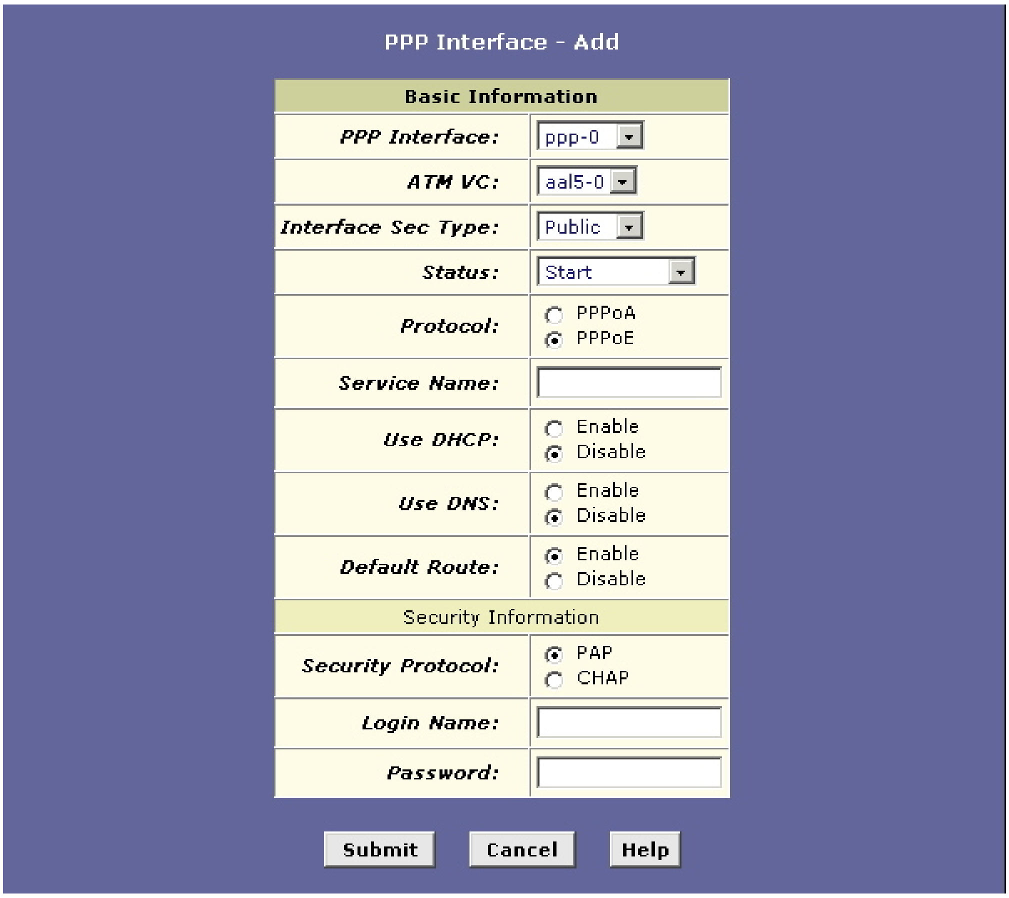
Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	0	35	LLC	2	

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 15: ATM VC Configuration

2 **Creating a PPP interface**:

a Select **Routing** > **PPP** > **Add** to add a new PPP interface:



PPP Interface - Add

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
Interface Sec Type:	Public
Status:	Start
Protocol:	○ PPPoA ● PPPoE
Service Name:	
Use DHCP:	○ Enable ● Disable
Use DNS:	○ Enable ● Disable
Default Route:	● Enable ○ Disable
Security Information	
Security Protocol:	● PAP ○ CHAP
Login Name:	
Password:	

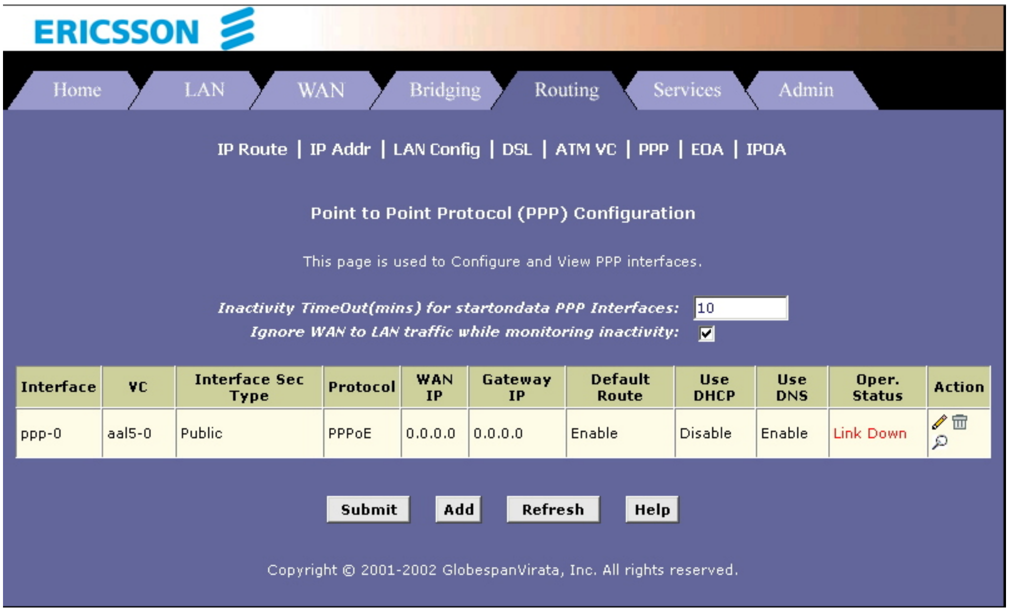
Figure 16: PPP Interface - Add

b Enter the provided fields as below:

Field	**Description**
PPP Interface	Select a PPP interface from the available interfaces, e.g. **ppp-0** .
ATM VC	Select the ATM VC you created in step 1, e.g. **aal5-0** .
IPF Type	**Public**
Status	Select **Start** or **StartOnData** **Start** - To establish connection whenever you turn on the HM210dp/di. **StartOnData** - To establish a connection whenever the device gets a request to connect to the Internet, such as when you open a browser requesting for web pages.
Protocol	**PPPoA** or **PPPoE** as required by your ISP.
Service Name	For **PPPoA** no need to set up. For **PPPoE** enter the Service Name if this is required by your ISP. Otherwise leave it blank.
Use DHCP	Select **Disable** unless your ISP instructs you to enable this service.
Use DNS	**Enable**
Default Route	**Enable**
Security Protocol	Select **PAP** or **CHAP** as required by your ISP.
Login Name/Password	The login name and password given by your ISP. **Note** that characters of colon (:), semicolon (;) and question mark (?) are not allowed when entering login name and password.

After entering the fields above, click **Submit**.

c You will return to the **PPP Configuration** page and see the new PPP interface. The "Oper. Status" column indicates if the link is currently up or down.



ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
IP Route | IP Addr | LAN Config | DSL | ATM VC | PPP | EOA | IPOA

Point to Point Protocol (PPP) Configuration

This page is used to Configure and View PPP interfaces.

Inactivity TimeOut(mins) for startondata PPP Interfaces: 10

Ignore WAN to LAN traffic while monitoring inactivity: ☑

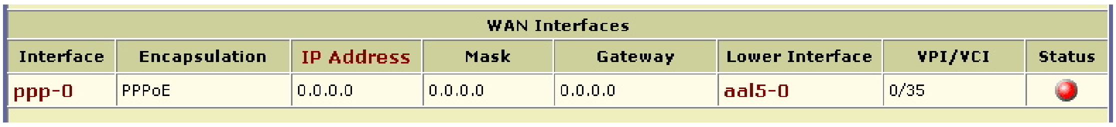
Interface	VC	Interface Sec Type	Protocol	WAN IP	Gateway IP	Default Route	Use DHCP	Use DNS	Oper. Status	Action
ppp-0	aal5-0	Public	PPPoE	0.0.0.0	0.0.0.0	Enable	Disable	Enable	Link Down	✎ 🗑 🔍

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 17: PPP Configuration

5.2.2 Check Your Connection Status

Select **Home** > **System Mode**. The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection.



WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoE	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	0/35	●

Figure 18: WAN IF Status

5.2.3 Configuring the PC

Keep your PC's setting as a DHCP client. No further configuration is required.

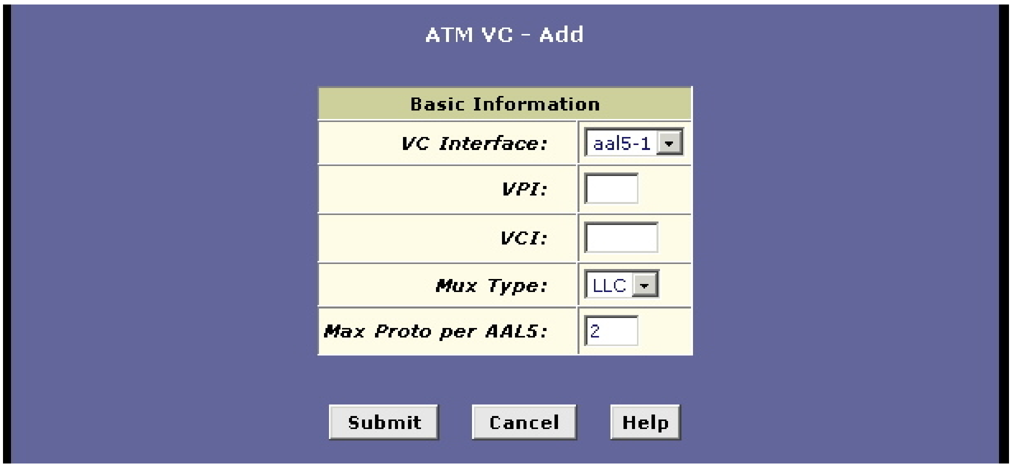
5.3 Router Connection Mode

This section describes both **RFC1577** and **RFC1483 Router** connection methods.

5.3.1 Configuring the HM210dp/di

1 **Creating an ATM VC interface**:

a Select **Bridging** > **ATM VC** > **Add**. The **ATM VC - Add** page appears:



ATM VC - Add

Basic Information	
VC Interface:	aal5-1
VPI:	
VCI:	
Mux Type:	LLC
Max Proto per AAL5:	2

Figure 19: ATM VC - Add

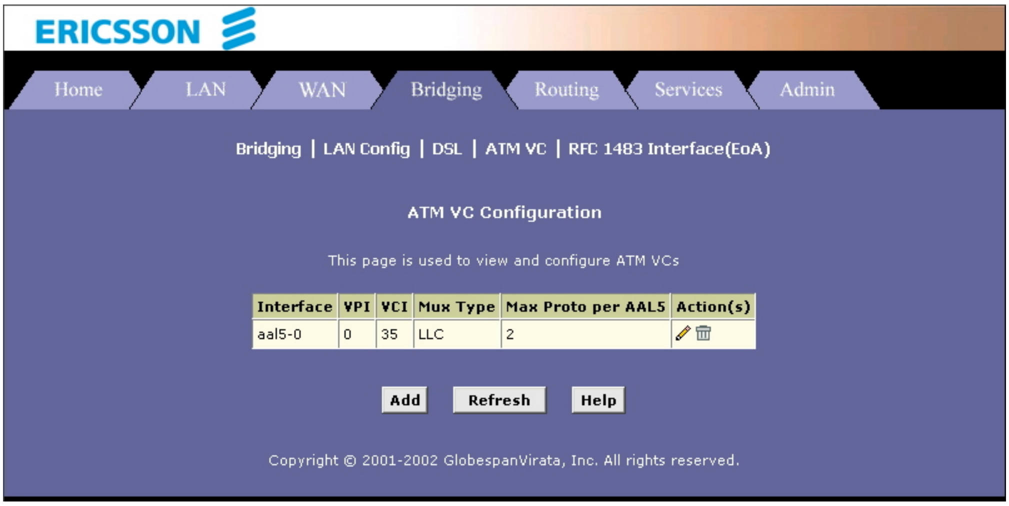
b Enter the provided fields as below:

Field	Description
VC Interface	Select a VC interfacce from the available interfaces, e.g. **aal5-0** .
VPI/VCI	Enter the VPI/VCI values given by your ISP, e.g. **0/34**
Mux Type	Select **LLC** or **VC** as required by your ISP.
Max Proto per AAL5	Keep the default **2**.

After entering the fields above, click **Submit**.

c When the confirmation page appears, click **Close**.

d You will return to the **ATM VC Configuration** table and see the newly added ATM VC entry.



ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)

ATM VC Configuration

This page is used to view and configure ATM VCs

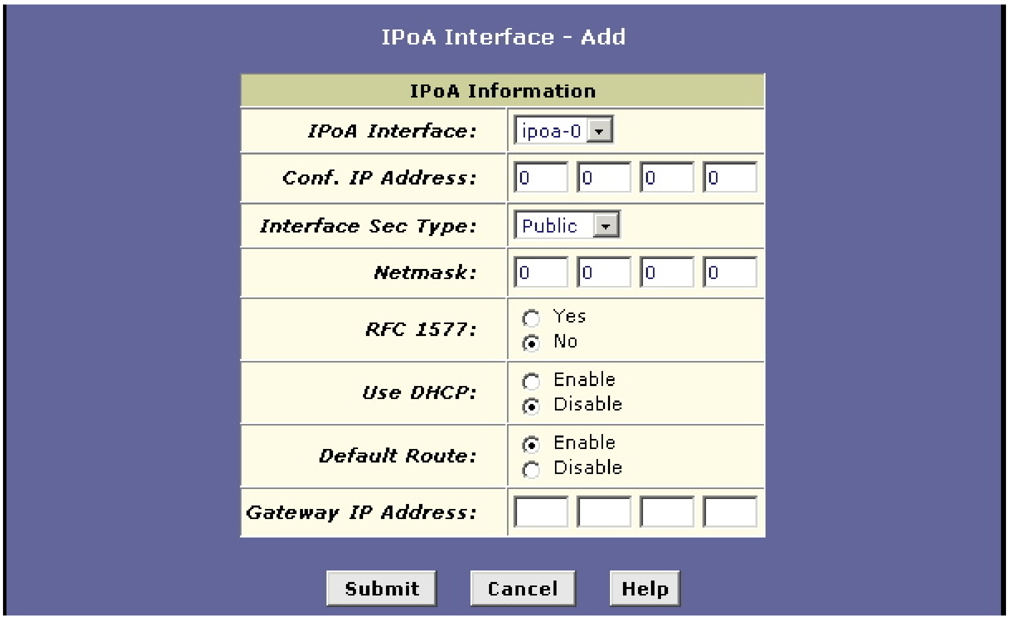
Interface	VPI	VCI	Mux Type	Max Proto per AAL5	Action(s)
aal5-0	0	35	LLC	2	✎ 🗑

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 20: ATM VC Configuration

2 **Creating a IPoA interface**:

a Select **WAN** > **IPoA** > **Add** to add a new IPoA interface:



IPoA Interface - Add

IPoA Information	
IPoA Interface:	ipoa-0
Conf. IP Address:	0 . 0 . 0 . 0
Interface Sec Type:	Public
Netmask:	0 . 0 . 0 . 0
RFC 1577:	○ Yes ● No
Use DHCP:	○ Enable ● Disable
Default Route:	● Enable ○ Disable
Gateway IP Address:	

Figure 21: IPoA Interface - Add

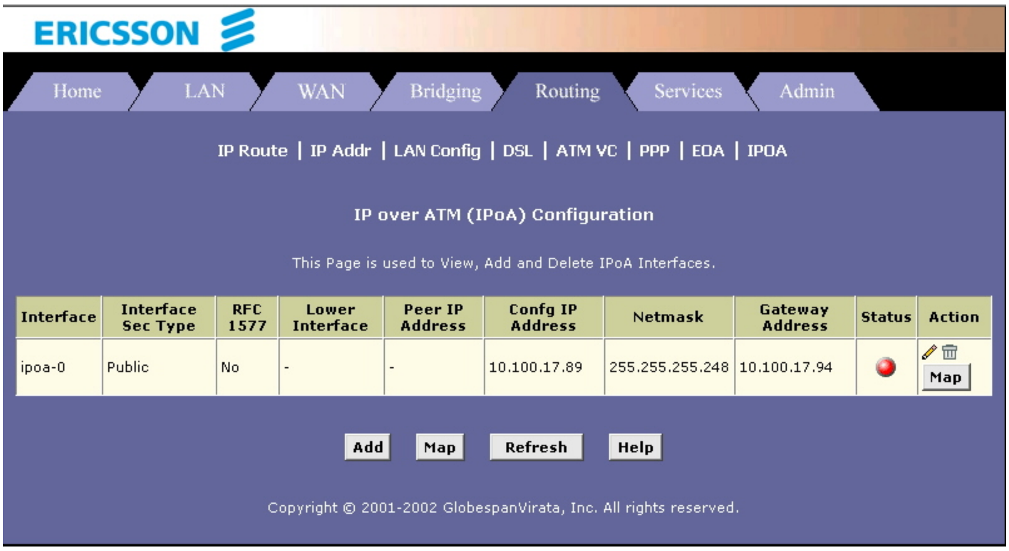
b Enter the provided fields as below:

Field	Description
IPoA Interface	Select an IPoA interface from the available interfaces, e.g. **ipoa-0** .
Conf. IP address	Enter the IP address given by your ISP, e.g. **10.100.17.89**
Interface Sec Type	Select Public, Private or DMZ
Netmask	Enter the IP address given by your ISP, e.g. **255.255.255.248**.
RFC 1577	For RFC 1577-Classical IP and ARP over ATM, select **Yes** For RFC 1483 Router, select **No.**
Use DHCP	
Default Route	**Enable**
Gateway IP Address	Enter the gateway IP address given by your ISP, e.g. **10.100.17.94**.

After entering the fields above, click the **Submit** button.

c When the confirmation page appears, click **Close**.

d You will return to the **IPoA Configuration** table and see the newly added IPoA entry.


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
IP Route | IP Addr | LAN Config | DSL | ATM VC | PPP | EOA | IPOA

IP over ATM (IPoA) Configuration

This Page is used to View, Add and Delete IPoA Interfaces.

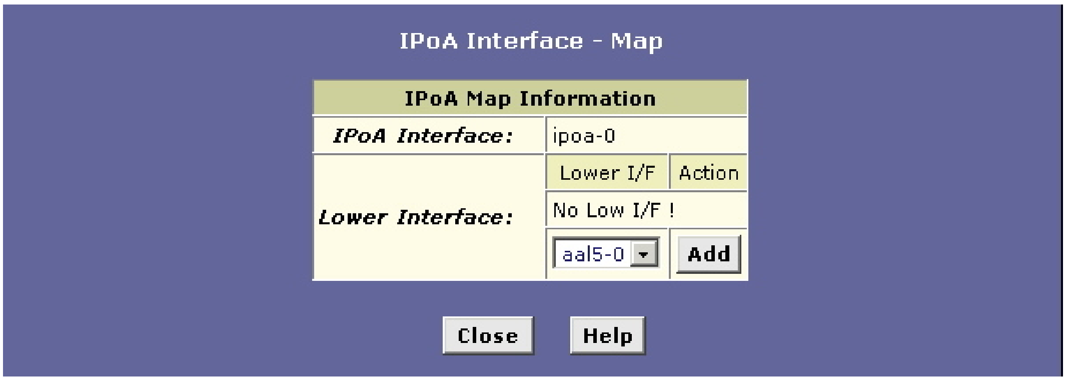
Interface	Interface Sec Type	RFC 1577	Lower Interface	Peer IP Address	Confg IP Address	Netmask	Gateway Address	Status	Action
ipoa-0	Public	No	-	-	10.100.17.89	255.255.255.248	10.100.17.94	●	✎ 🗑 Map

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 22: IPoA Configuration

3 **Mapping IPoA interface to a lower interface**:

In the **IPoA Configuration** table, locate the new IPoA entry and click **Map** in the "Action" column.



IPoA Interface - Map

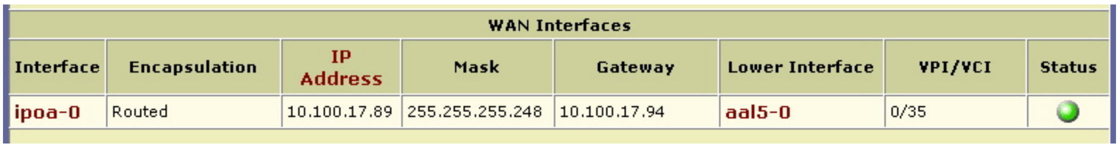
IPoA Map Information		
IPoA Interface:	ipoa-0	
Lower Interface:	Lower I/F	Action
	No Low I/F !	
	aal5-0 ▾	Add

Figure 23: IPoA Interface - Map

On **IPoA Interface - Map** page, from the drop-down list select the ATM VC you created in step 1 to be mapped to this IPoA interface and then click **Add**. Click **Close** to exit the confirmation page.

5.3.2 Check Your Connection Status

Select **Home** > **System Mode**. The WAN Interface item should display the interface you created to communicate with your ISP. A green ball in the Status field indicates a successful connection.



WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ipoa-0	Routed	10.100.17.89	255.255.255.248	10.100.17.94	aal5-0	0/35	●

Figure 24: WAN IF Status

5.3.3 Configuring the PC

Keep your PC's setting as a DHCP client. No further configuration is required.

6 Configuring IP Routes

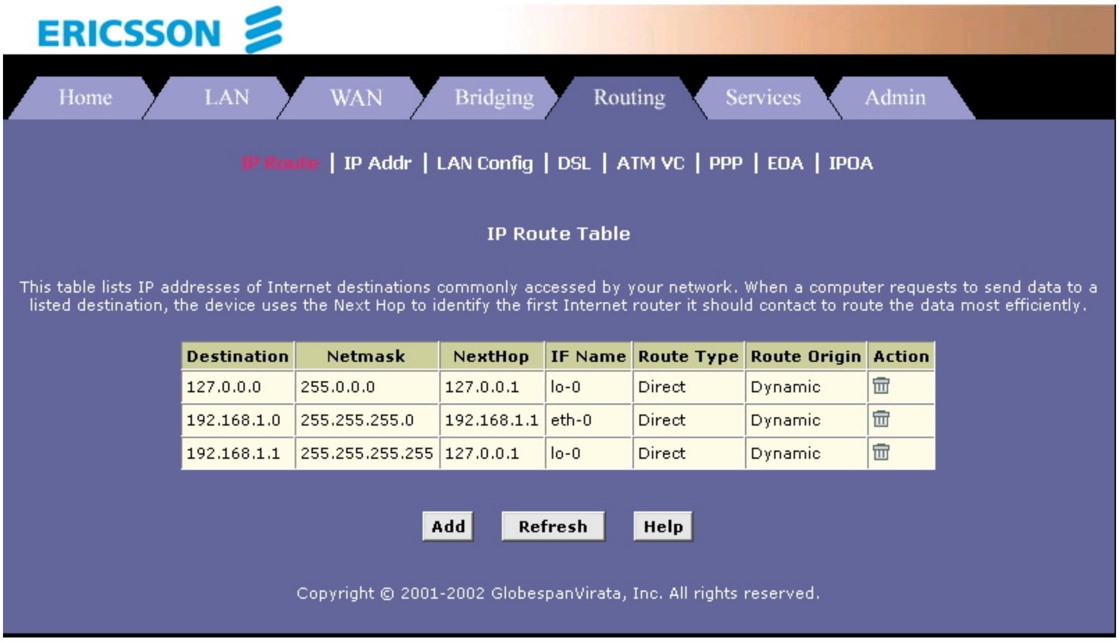
You can use the Configuration Manager to define specific routes for your Internet and network data. This chapter provides instructions for creating routes.

Most users do not need to define IP routes. You may need to define routes if:

- Your network setup includes two or more networks or subnets
- You connect to two or more ISP services
- You connect to a remote corporate LAN.

6.1 Viewing the IP Routing Table

To view the HM210dp/di routing table, select **Routing > IP Route**. The following page appears:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
IP Route | IP Addr | LAN Config | DSL | ATM VC | PPP | EOA | IPOA
Add
Refresh
Help

IP Route Table

This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.

Destination	Netmask	NextHop	IF Name	Route Type	Route Origin	Action
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	Dynamic	🗑
192.168.1.0	255.255.255.0	192.168.1.1	eth-0	Direct	Dynamic	🗑
192.168.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	🗑

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

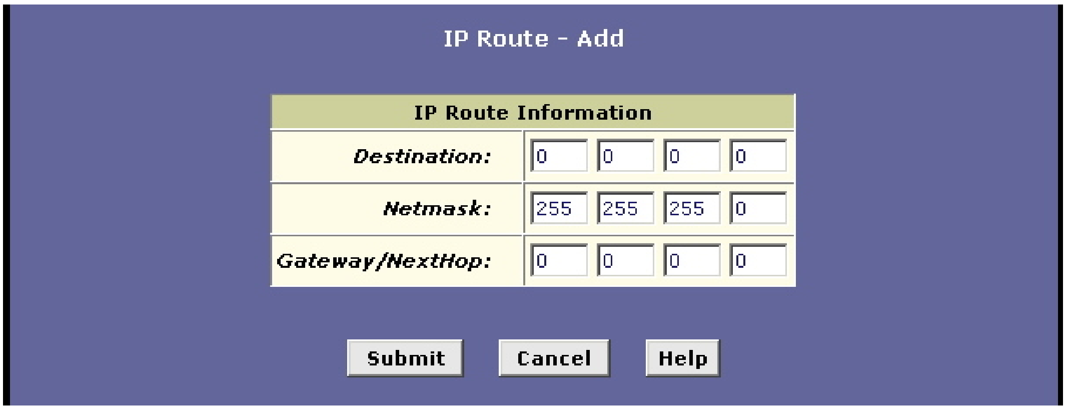
Figure 25: IP Route Table

The IP Route Table includes routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

6.2 Adding IP Routes

1 Select **Routing** > **IP Route** > **Add**. The **IP Route - Add** page appears:



IP Route - Add

IP Route Information

Destination:	0	0	0	0
Netmask:	255	255	255	0
Gateway/NextHop:	0	0	0	0

Figure 26: IP Route - Add

2 Specify the destination, network mask, and gateway or next hop for this route.

To create a route that defines the default gateway for your LAN, enter **0.0.0.0** in both the **Destination** and **Netmask** fields. Enter your ISP's IP address in the **Gateway/NextHop** field.

Note:

You cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.

3 Click the **Submit** button. The IP Routing Table will now display the new route.

4 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

7 DHCP Configuration

You can configure your network and HM210dp/di to use the Dynamic Host Configuration Protocol (DHCP). This chapter provides instructions for implementing DHCP on your network.

7.1 HM210dp/di DHCP Modes

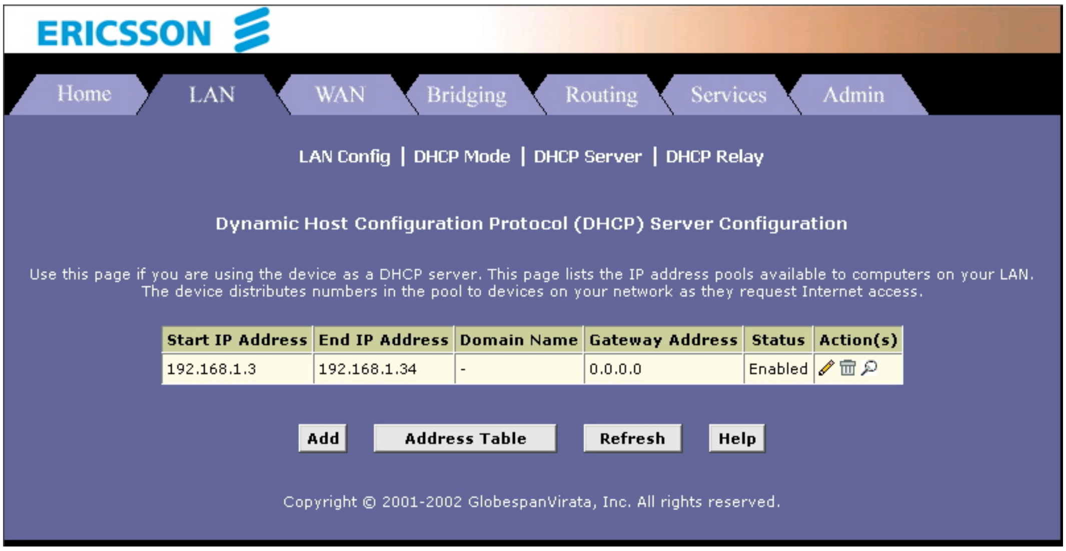
The HM210dp/di can be configured as a DHCP server, DHCP relay agent, or, in some cases, a DHCP client.

- **DHCP server** - It will maintain the pool of addresses and distribute them to your LAN computers. If the pool of addresses includes private IP addresses, you must also configure the Network Address Translation (NAT) service, so that the private addresses can be translated to your public IP address on the Internet. Both DHCP server and NAT are enabled in the default configuration.
- **DHCP relay agent** - If your ISP performs the DHCP server function for your network, then you can configure the device as a DHCP relay agent. When the HM210dp/di receives a request for Internet access from a computer on your network, it contacts your ISP for the necessary IP information, and then relays the assigned information back to the computer.
- **DHCP client** - If you have another PC or device on your network that is already performing the DHCP server function, you can configure the LAN port on the HM210dp/di to be a DHCP client of that server.

7.2 Configuring DHCP Server

7.2.1 Creating IP Address Pools

1 Select **LAN** > **DHCP Server**. The **DHCP Server Configuration** page appears:



Dynamic Host Configuration Protocol (DHCP) Server Configuration

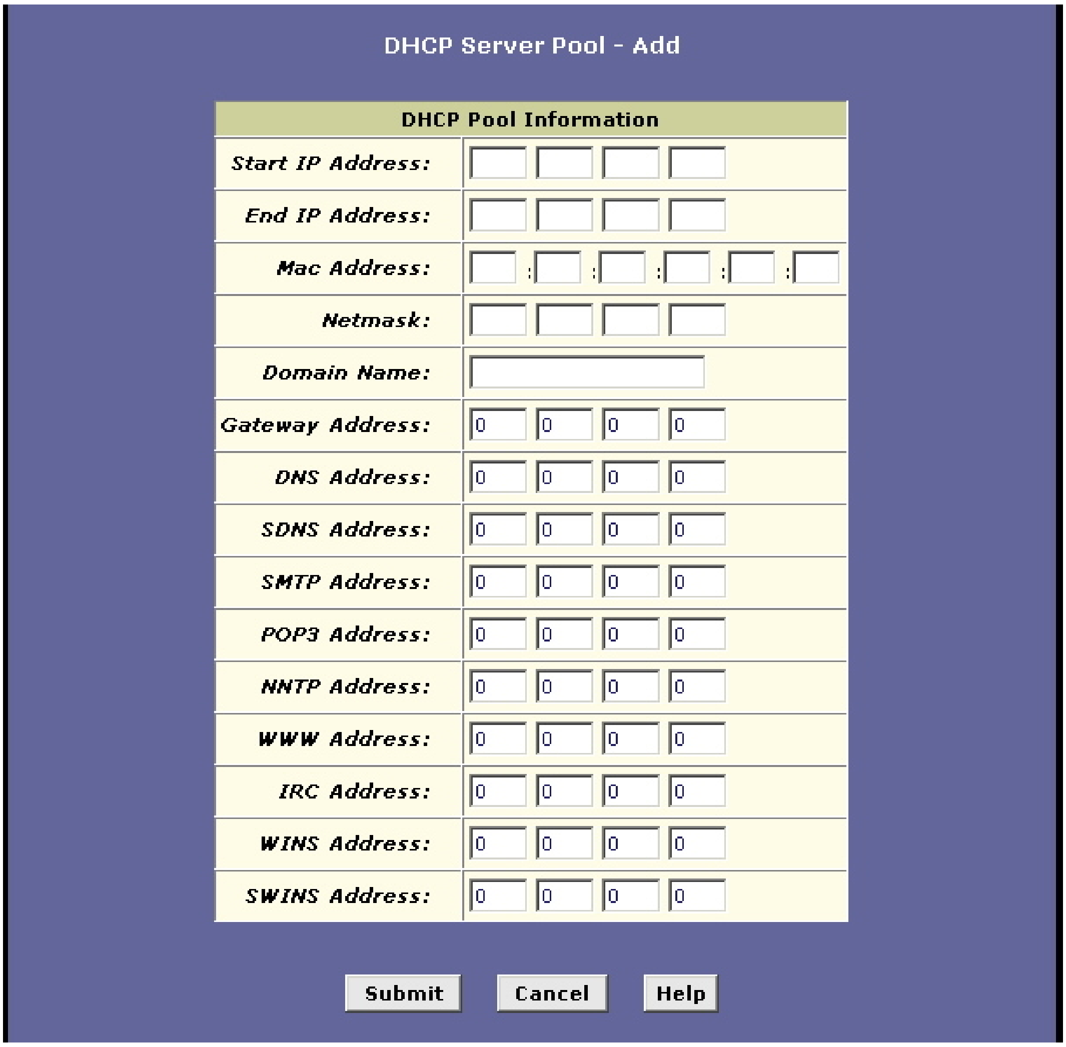
Use this page if you are using the device as a DHCP server. This page lists the IP address pools available to computers on your LAN. The device distributes numbers in the pool to devices on your network as they request Internet access.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
192.168.1.3	192.168.1.34	-	0.0.0.0	Enabled	✎ 🗑 🔍

Figure 27: DHCP Server Configuration page

Each pool you create displays in a row on the table on this page. You can create up to eight pools. Additional pools may be needed when the device is configured with multiple LAN interfaces.

2 To add an IP address pool, click **Add**. The **DHCP Server Pool - Add** page appears:



DHCP Server Pool - Add

DHCP Pool Information						
Start IP Address:						
End IP Address:						
Mac Address:	:	:	:	:	:	
Netmask:						
Domain Name:						
Gateway Address:	0	0	0	0		
DNS Address:	0	0	0	0		
SDNS Address:	0	0	0	0		
SMTP Address:	0	0	0	0		
POP3 Address:	0	0	0	0		
NNTP Address:	0	0	0	0		
WWW Address:	0	0	0	0		
IRC Address:	0	0	0	0		
WINS Address:	0	0	0	0		
SWINS Address:	0	0	0	0		

Figure 28: DHCP Server Pool - Add

The **Start IP Address**, **End IP Address**, **Net Mask** and **Gateway Address** fields are required, the others are optional.

Field	Description
Start/End IP Addresses	Specify the lowest and highest IP addresses in the pool.
Mac Address	Allows you to assign a specific IP address to a specific computer, identified by this MAC address. If this is the case, you must have specified the same IP address in both the Start/End IP Address fields.
Netmask	Specifies the associated subnet mask of the IP address in this range.
Domain Name	The domain name to be used by DHCP clients.
Gateway Address	The address of the default gateway. Typically, it is the device's LAN port IP address.
DNS	The IP address of the DNS Server. Its typically located with your ISP.

Field	Description
SDSN ... SWINS (optional)	The IP addresses of devices that perform various services for DHCP clients.

3 Click the **Submit** button. A configuration page appears to indicate that the pool has been added successfully.

4 Click **Close** to return to the **DHCP Configuration** page.

7.2.2 Enabling DHCP Server Mode

1 Select **LAN** > **DHCP Mode**, and from the "DHCP Mode" drop-down list select **DHCP Server**. Click the **Submit** button.

A page appears to confirm the change.

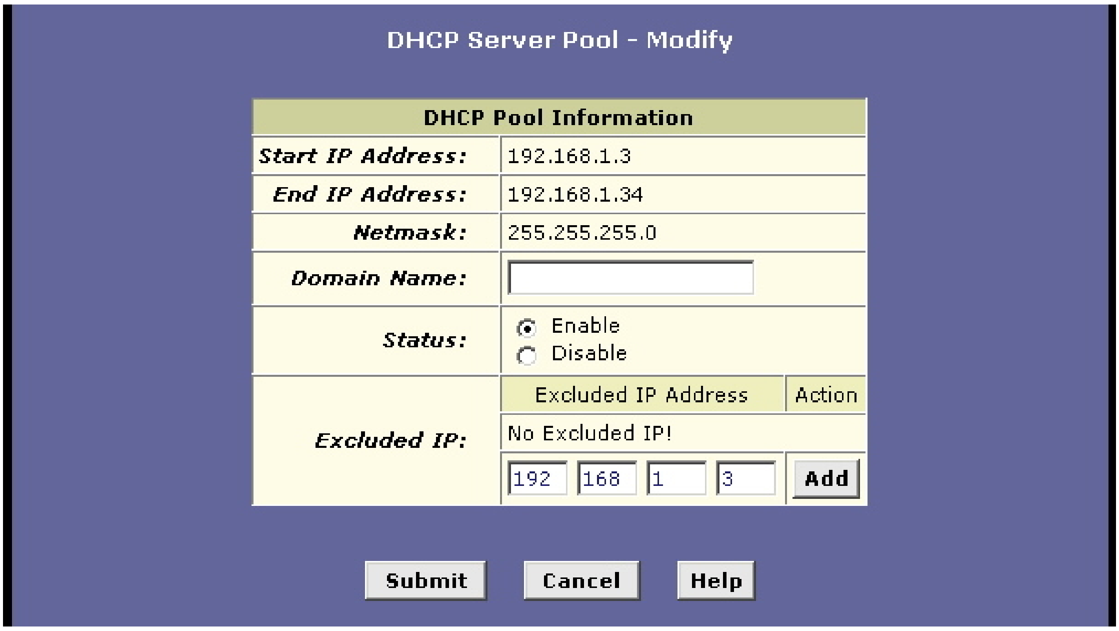
2 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

7.2.3 Configuring Your PCs as DHCP Clients

For each computer that you want to configure to receive IP information automatically, configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system). Refer to section 3.1 - "Configuring your PCs as DHCP Clients" for detailed instructions.

7.2.4 Modifying IP Address Pools

Select **LAN** > **DHCP Server** and then click the **modify** icon on the DHCP pool which you want to modify. The **DHCP Server Pool - Modify** page appears:



DHCP Server Pool - Modify

DHCP Pool Information	
Start IP Address:	192.168.1.3
End IP Address:	192.168.1.34
Netmask:	255.255.255.0
Domain Name:	
Status:	● Enable ○ Disable
Excluded IP:	Excluded IP Address / Action No Excluded IP! 192 168 1 3 Add

Figure 29: DHCP Server Pool - Modify

When modifying an address pool, you are **only** allowed to:

- Change the domain name associated with the pool.

- Exclude IP addresses within its range from distribution. To exclude an IP address, enter it in the field provided and click **Add**.

If you want to change other attributes, you must delete the pool and create a new one.

After entering your changes, click the**Submit** button.

Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

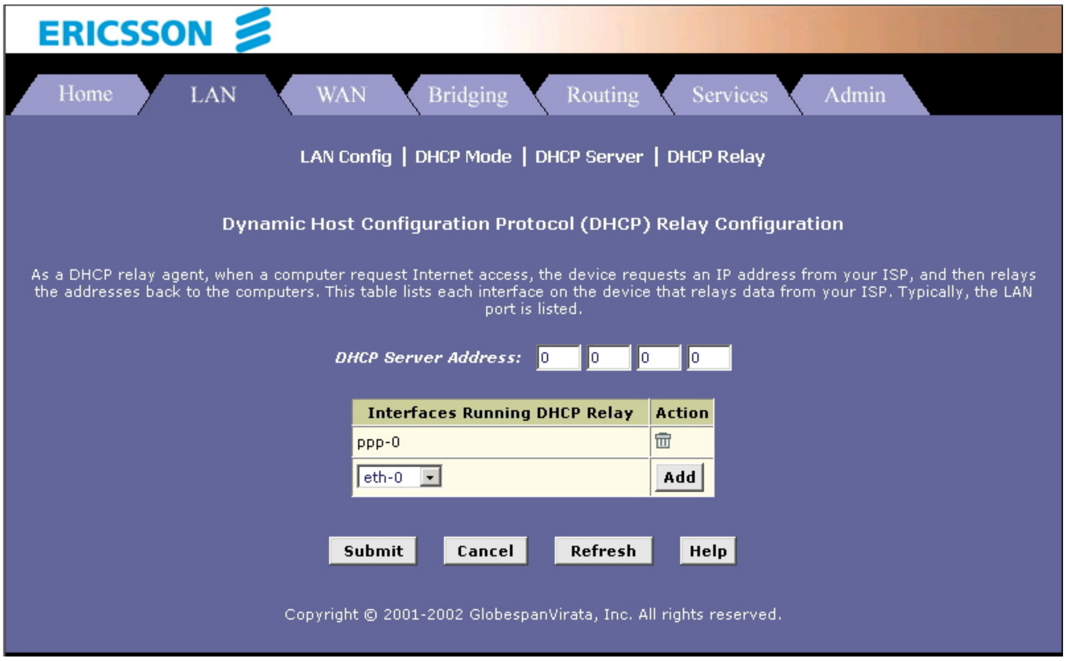
7.2.5 Viewing Current DHCP Address Assignments

To view a table of all current IP address assignments, select **LAN** > **DHCP Server** > **Address Table**.

7.3 Configuring DHCP Relay

7.3.1 Defining the DHCP Relay Interface(s)

1 Select **LAN** > **DHCP Relay**. The **DHCP Relay Configuration** page appears:



Dynamic Host Configuration Protocol (DHCP) Relay Configuration

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.

DHCP Server Address: 0 . 0 . 0 . 0

Interfaces Running DHCP Relay	Action
ppp-0	🗑
eth-0 ▾	Add

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 30: DHCP Relay Configuration page

This page provides a text box for entering the IP address of your ISP's DHCP server and a table that lists the interfaces on your HM210dp/di that can relay DHCP information.

2 Type the IP address of your ISP's DHCP server in the fields provided.

If you do not have this address, it is not essential to enter it. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

3 If the interface named **eth-0** is not already displaying, select it from the drop-down list and click **Add**.

4 Click the **Submit** button. A page appears to confirm your changes.

7.3.2 Enabling DHCP Relay Mode

1 Select **LAN > DHCP Mode** and from the "DHCP Mode" drop-down list select **DHCP Relay**. Click the **Submit** button.

A page appears to confirm the change.

2 Select **Admin > Commit & Reboot** and click **Commit** to save your changes to permanent storage.

7.3.3 Configuring Your PCs as DHCP Clients

For each computer that you want to configure to receive IP information automatically, configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system). Refer to section 3.1 - "Configuring your PCs as DHCP Clients" for detailed instructions.

8 NAT Configuration

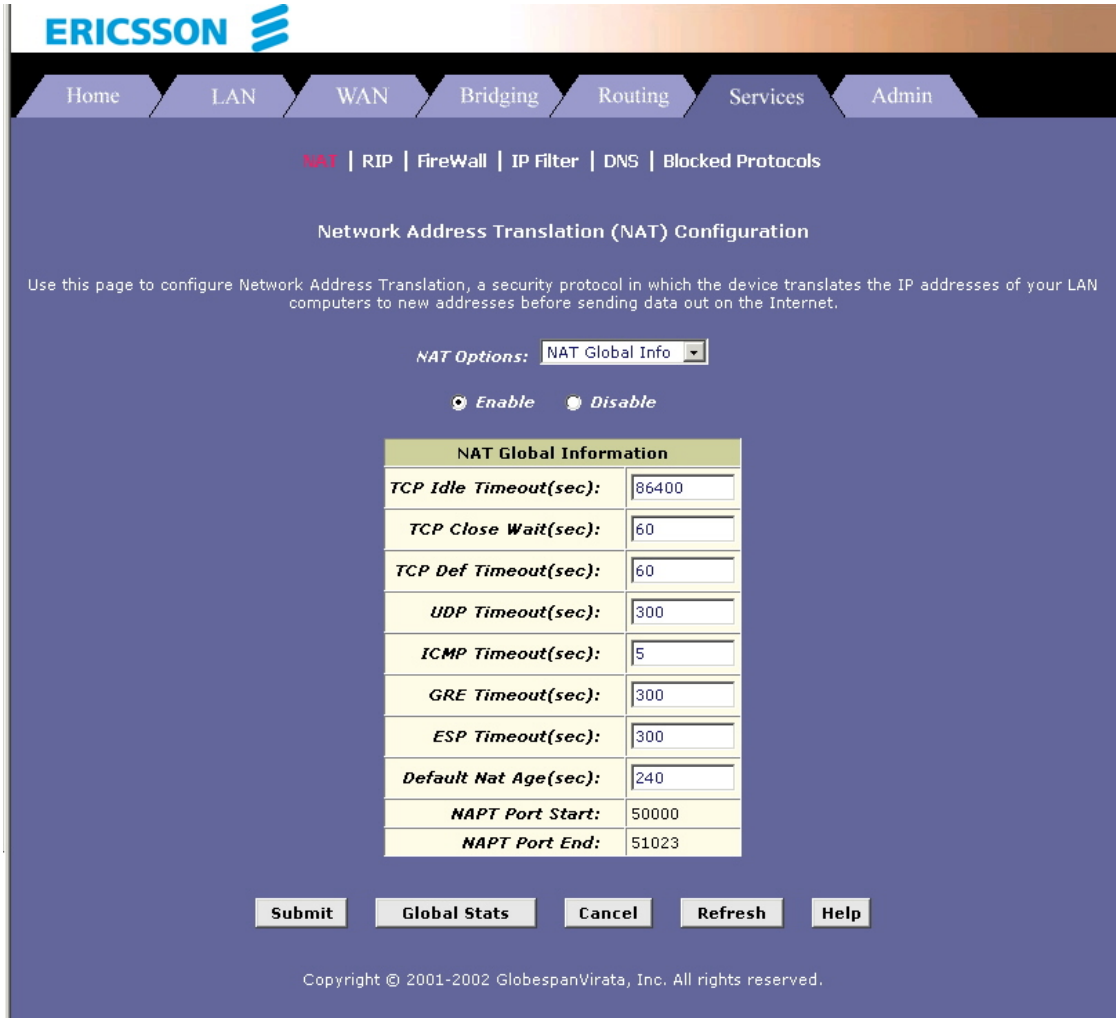
This chapter provides an overivew of Network Address Translation (NAT) and instructions for modifying the default configuration on your HM210dp/di.

8.1 Default NAT Setup

By default, NAT is enabled, with an Network Address Port Translation (NAPT) rule configured that translates any private address on the LAN side to your ISP-assigned public IP address on the WAN side.

8.2 Viewing NAT Configuration

To view your NAT settings, select **Services > NAT**. The **NAT Configuration** page appears:



Network Address Translation (NAT) Configuration

Use this page to configure Network Address Translation, a security protocol in which the device translates the IP addresses of your LAN computers to new addresses before sending data out on the Internet.

NAT Options: NAT Global Info

● *Enable* ○ *Disable*

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	5
GRE Timeout(sec):	300
ESP Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	51023

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 31: NAT Configuraiton

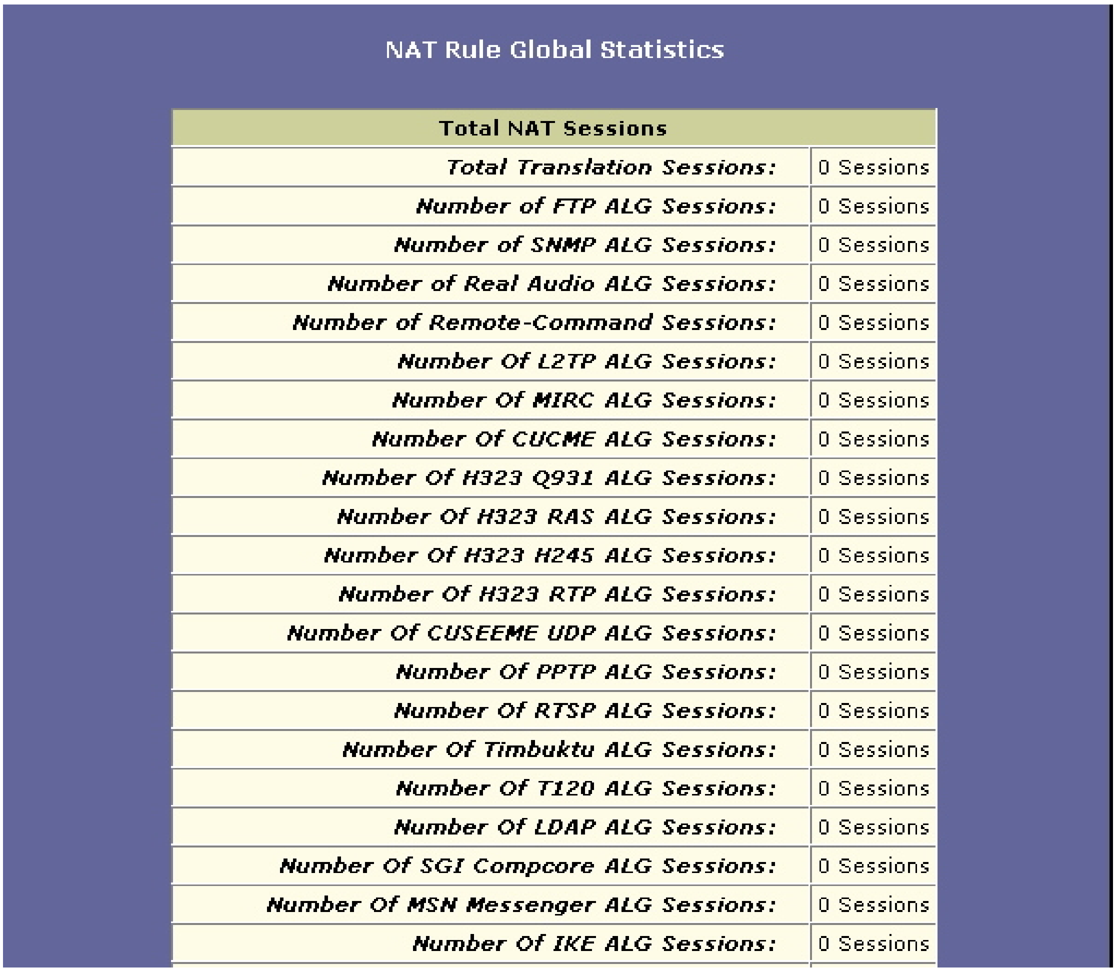
The NAT Global information table contains the following fields:

Field	Description
TCP Idle Timeout (sec)	When a NAT rule is in effect on a TCP session in the active state, the session will timeout if no packets are received for the specified time.

Field	Description
TCP Close Wait (sec)	When in the TCP session's closing state, the session will timeout if no packets are received for the specified time.
TCP Def Timeout (sec)	When in the TCP session's establishing state, the session will timeout if no packets are received for the specified time.
UDP Timeout (sec)	Same as TCP Idle Timeout, but for UDP packets.
ICMP Timeout (sec)	Same as TCP Idle Timeout, but for ICMP packets.
GRE Timeout (sec)	Same as TCP Idle Timeout, but for GRE packets.
Default NAT Age (sec)	For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.
NAPT Port Start/End	When an NAPT rule is defined, the source ports will be translated to sequential numbers in this range.

If you change any values, click **Submit**, and then commit your changes to permanent system memory.

You can click **Global Stats** to view accumulated data on how many NAT rules have been invoked and how much data has been translated. A page similar to the one below is displayed:



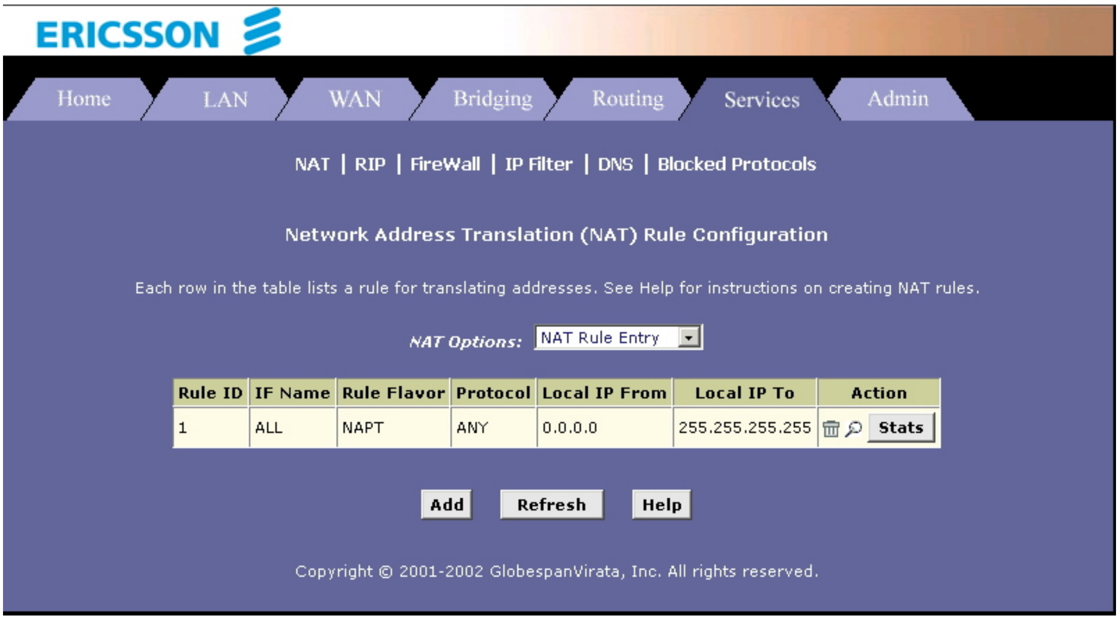
NAT Rule Global Statistics

Total NAT Sessions	
Total Translation Sessions:	0 Sessions
Number of FTP ALG Sessions:	0 Sessions
Number of SNMP ALG Sessions:	0 Sessions
Number of Real Audio ALG Sessions:	0 Sessions
Number of Remote-Command Sessions:	0 Sessions
Number Of L2TP ALG Sessions:	0 Sessions
Number Of MIRC ALG Sessions:	0 Sessions
Number Of CUCME ALG Sessions:	0 Sessions
Number Of H323 Q931 ALG Sessions:	0 Sessions
Number Of H323 RAS ALG Sessions:	0 Sessions
Number Of H323 H245 ALG Sessions:	0 Sessions
Number Of H323 RTP ALG Sessions:	0 Sessions
Number Of CUSEEME UDP ALG Sessions:	0 Sessions
Number Of PPTP ALG Sessions:	0 Sessions
Number Of RTSP ALG Sessions:	0 Sessions
Number Of Timbuktu ALG Sessions:	0 Sessions
Number Of T120 ALG Sessions:	0 Sessions
Number Of LDAP ALG Sessions:	0 Sessions
Number Of SGI Compcore ALG Sessions:	0 Sessions
Number Of MSN Messenger ALG Sessions:	0 Sessions
Number Of IKE ALG Sessions:	0 Sessions

Figure 32: NAT Rule Global Statistics page

8.3 Viewing NAT Rules and Rule Statistics

To view the NAT Rules currently defined on your system, select **Services > NAT > NAT Rule Entry**. The **NAT Rule Configuration** page appears:



Network Address Translation (NAT) Rule Configuration

Each row in the table lists a rule for translating addresses. See Help for instructions on creating NAT rules.

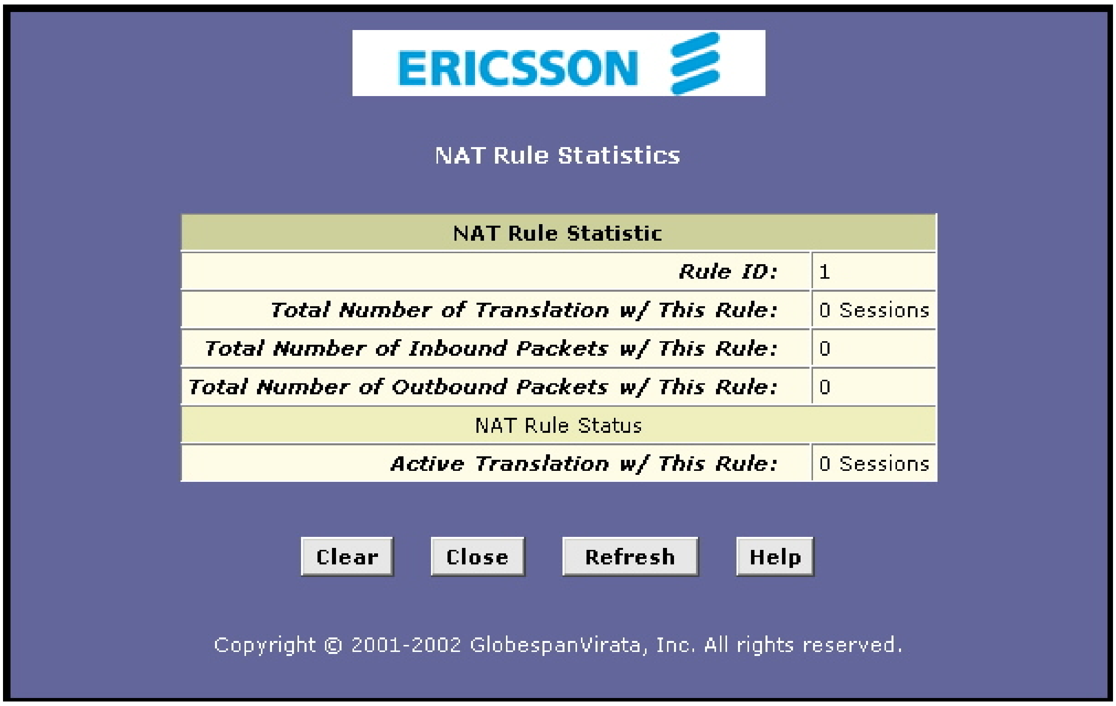
NAT Options: NAT Rule Entry

Rule ID	IF Name	Rule Flavor	Protocol	Local IP From	Local IP To	Action
1	ALL	NAPT	ANY	0.0.0.0	255.255.255.255	Stats

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 33: NAT Rule Configuration page

To view data on how often a specific NAT rule has been used, click **Stats** in the Action column. A page similar to the one below appears:



NAT Rule Statistics

NAT Rule Statistic	
Rule ID:	1
Total Number of Translation w/ This Rule:	0 Sessions
Total Number of Inbound Packets w/ This Rule:	0
Total Number of Outbound Packets w/ This Rule:	0
NAT Rule Status	
Active Translation w/ This Rule:	0 Sessions

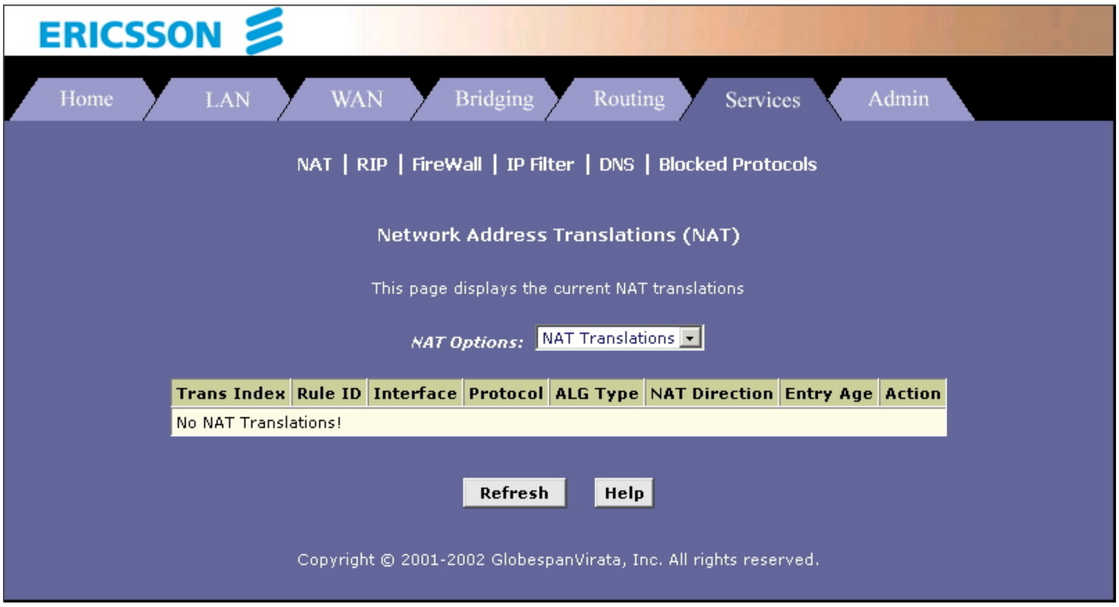
Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 34: NAT Rule Statistics page

The statistics show how many times this rule has been invoked and how many curently active sessions are using this rule.

8.4 Viewing Current NAT Translations

To view a list of NAT translations that have recently been performed and which remain in effect (for any of the defined rules), select **Services > NAT > NAT Translations**. The **NAT Translations** page appears:



Network Address Translations (NAT)

This page displays the current NAT translations

NAT Options: NAT Translations

Trans Index	Rule ID	Interface	Protocol	ALG Type	NAT Direction	Entry Age	Action
No NAT Translations!							

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 35: NAT Translations

For each current NAT translation session, the table contains the following fields:

Field	**Description**
Trans Index	The sequential number assigned to the IP session used by this NAT translation session.
Rule ID	The ID of the NAT rule invoked.
Interface	The device interface on which the NAT rule was invoked (from the rule definition).
Protocol	The IP protocol used by the data packets that are undergoing translations (from the rule definition). Example: TCP, UDP, ICMP.
Alg Type	The Application Level Gateway (ALG), if any, that was used to enable this NAT translation. (ALGs are special settings that certain applications require in order to work while NAT is enabled).
NAT Direction	The direction (incoming or outgoing) of the translation (from the port definition).
Entry Age	The elapsed time, in seconds, of the NAT translation session.

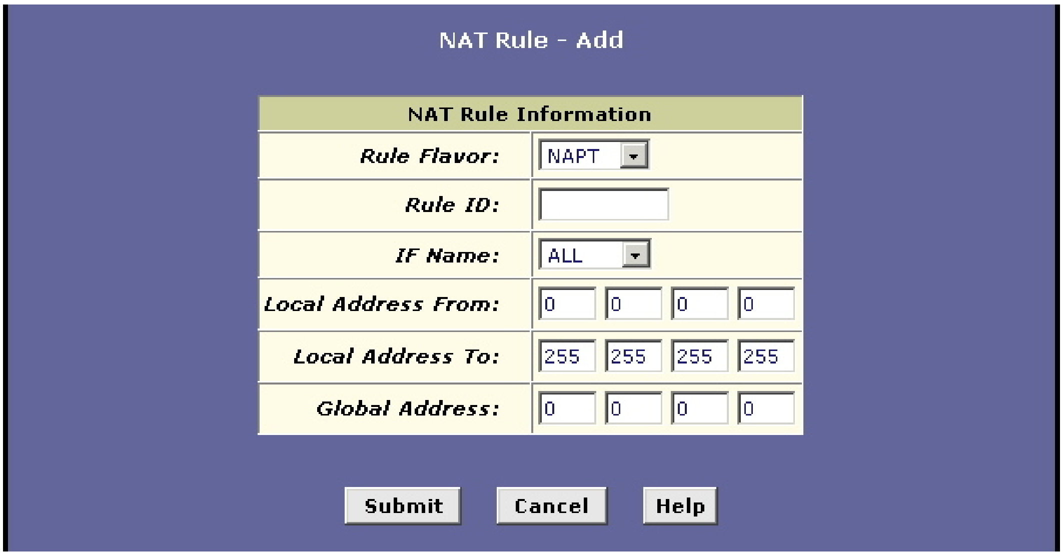
8.5 Adding NAT Rules

This section explains how to create rules for the various NAT flavors.

8.5.1 The NAPT Rule

The NAT flavor NAPT was used in your default configuration. The NAPT flavor translates all LAN-side private source IP addresses to a single public IP address. It also translates the source port numbers to port numbers that are defined on the **NAT Global Configuration** page.

1 Select **Services** > **NAT** > **NAT Rule Entry** > **Add**.



NAT Rule - Add

NAT Rule Information				
Rule Flavor:	NAPT			
Rule ID:				
IF Name:	ALL			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address:	0	0	0	0

Figure 36: Nat Rule NAPT - Add

2 In the "Rule Flavor" drop-down list, select **NAPT**.

3 In the "Rule ID" field, type an ID for the rule.

The Rule ID determines the order in which the rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4 From the "IF Name" drop-down list, select the interface on the HM210dp/di to which this rule applies.

Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5 In the **Local Address From/To** fields, type the starting and ending IP addresses, respectively, of the range of private addresses you want to be translated. Or, type the same address in both fields to specify a single IP address.

If all LAN IP addresses should be translated, specify 0.0.0.0 and 255.255.255.255 respectively.

6 In the **Global Address** field, typethe address that you want to serve as the publicly known address for the LAN computer.

7 When you have completed entering all information, click the **Submit** button. A page appears to confirm the change.

8 Click **Close** to return to the **NAT Configuration** page. The new rule should now be displayed in the NAT Rule table.

9 On the **NAT Configuration** page, ensure that the **Enable** radio button is selected.

10 On the **NAT Configuration** page, click the **Submit** button. A page appears to confirm your changes.

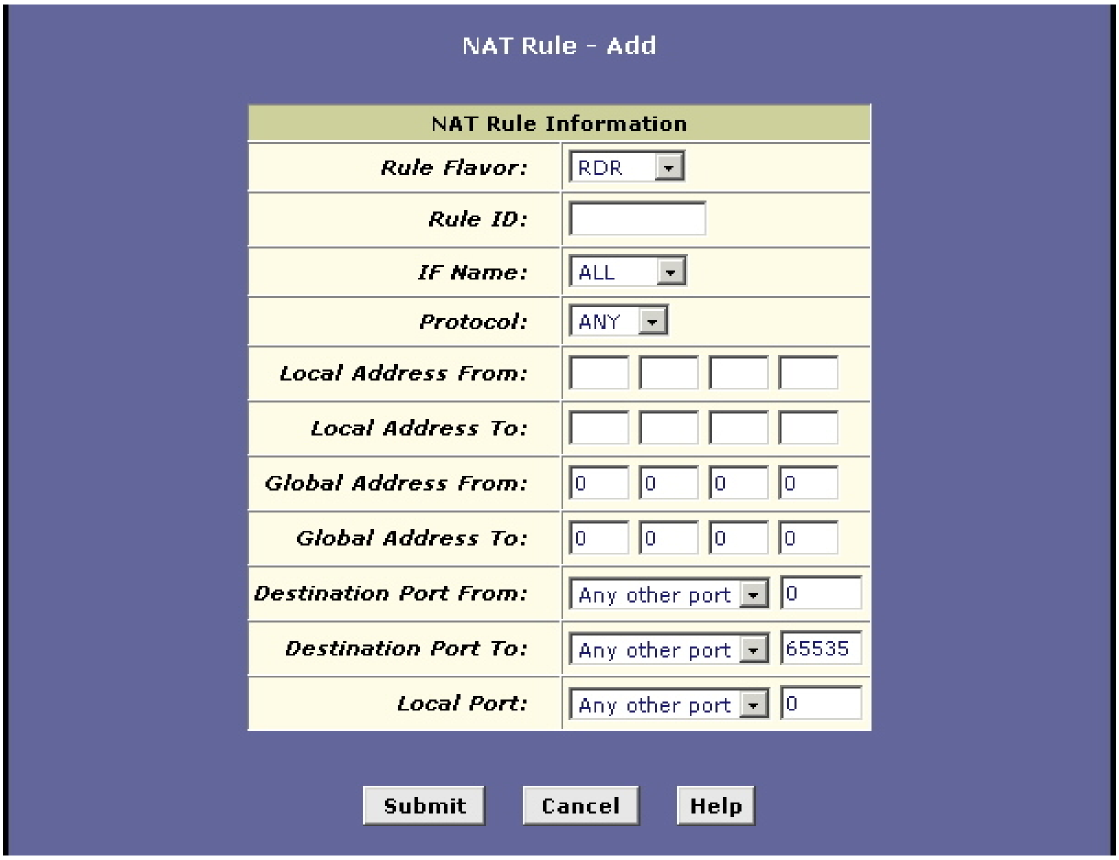
11 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

8.5.2 The RDR Rule

You can create an RDR rule to make a computer on your LAN, such as a Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer's private IP address is translated to your public IP address in all incoming and outgoing data packets.

Note:

Without an RDR rule (or BIMAP rule), the HM210dp/di blocks attempts by external computers to access your LAN computers.



NAT Rule - Add

NAT Rule Information

Rule Flavor:	RDR
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	
Local Address To:	
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535
Local Port:	Any other port 0

Figure 37: NAT Rule RDR - Add

Follow these instructions to add an RDR rule:

1 Display the **NAT Rule - Add** page, select **RDR** as the Rule Flavor and type a Rule ID.

2 Select the interface on the HM210dp/di to which this rule applies.

3 Select a protocol to which this rule applies, or choose **ALL** if the rule applies to all data.

4 In the **Local Address From/To** fields, type the same private IP address, or the lowest and highest IP addresses in a range:

If you type the same IP address in both fields, incoming traffic that matches the criteria of this rule will be redirected to that IP address.

If you type a range of IP addresses, incoming traffic will be redirected to any available computer in that range. This option would typically be used for load balancing, whereby traffic is distributed among several redundant servers.

5 In the **Global Address From/To** fields, type the public IP address assigned to you by your ISP.

If you have multiple WAN interfaces, in both fields type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on WAN interfaces not specified here.

If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range.

6 Enter a destination port ID (or a range) as criteria for incoming traffic.

Enter a starting and ending port number in the **Destination Port From/To** fields if incoming traffic destined for these port types should be redirected to the address(es) specified in step 3. Or, enter the same addres in both fields.

7 If the publicly accessible LAN computer uses a non-standard port number for the type of traffic it receives, type the non-standard port number in the **Local Port** field.

8 When you have completed entering all information, click the **Submit** button. A page appears to confirm the change.

9 Click **Close** to return to the **NAT Configuration** page. The new rule should now be displayed in the NAT Rule table.

10 On the **NAT Configuration** page, ensure that the **Enable** radio button is selected.

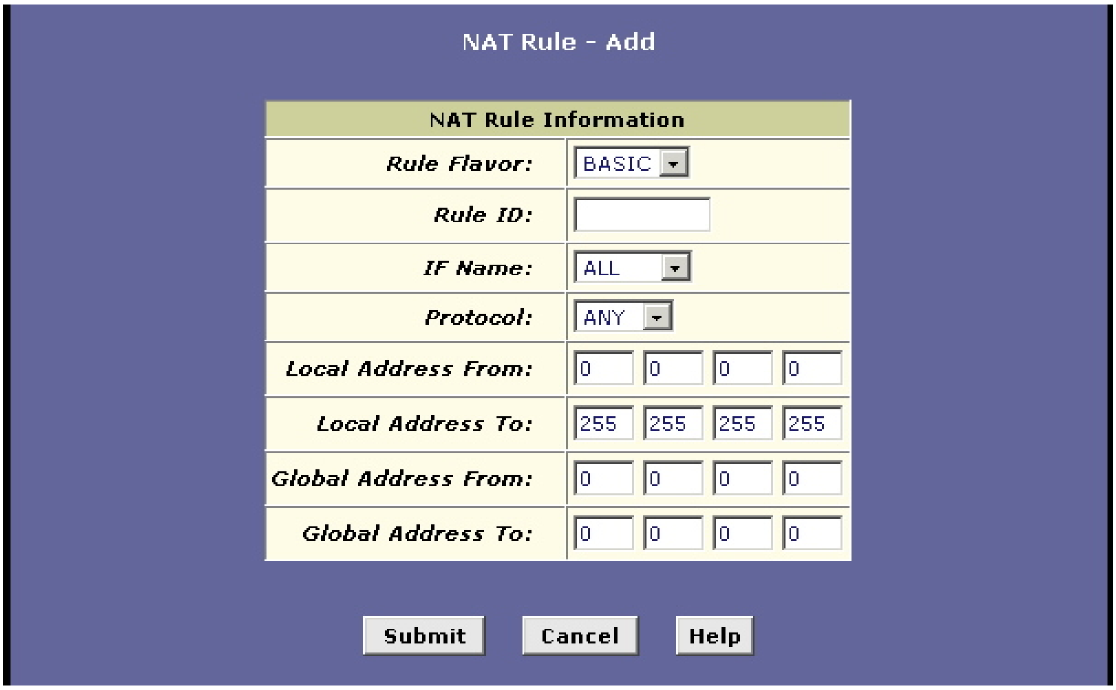
11 On the **NAT Configuration** page, click the **Submit** button. A page appears to confirm your changes.

12 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

8.5.3 The BASIC Rule

The BASIC flavor translates the private (LAN-side) IP address to a public (WAN-side) IP address, like the NAPT rule. However, unlike the NAPT rule, the BASIC rule do not translate the port number in the packet header; they are passed through untranslated. Therefore, the BASIC rule does not provide the same level of security as the NAPT rule.

The figure below shows the fields used for adding a BASIC rule:



NAT Rule - Add

NAT Rule Information	
Rule Flavor:	BASIC
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0

Figure 38: NAT Rule BASIC - Add

1 Display the **NAT Rule - Add** page, select **BASIC** as the Rule Flavor and type a Rule ID.

2 Select the interface and, if desired, a protocol that this rule applies to.

3 In the **Local Address From/To** fields, type the starting and ending IP addresses that identify the range of private addresses you want to be translated. Or, type the same IP address in both fields.

If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 4).

4 In the **Global Address From/To** fields, type the starting and ending IP address that identify the pool of public IP addresses to which to translate your private addresses. Or, type the same IP address in both fields (if you also specified a single address in step 3).

5 When you have completed entering all information, click the **Submit** button. A page appears to confirm the change.

6 Click **Close** to return to the **NAT Configuration** page. The new rule should now be displayed in the NAT Rule table.

7 On the **NAT Configuration** page, ensure that the **Enable** radio button is selected.

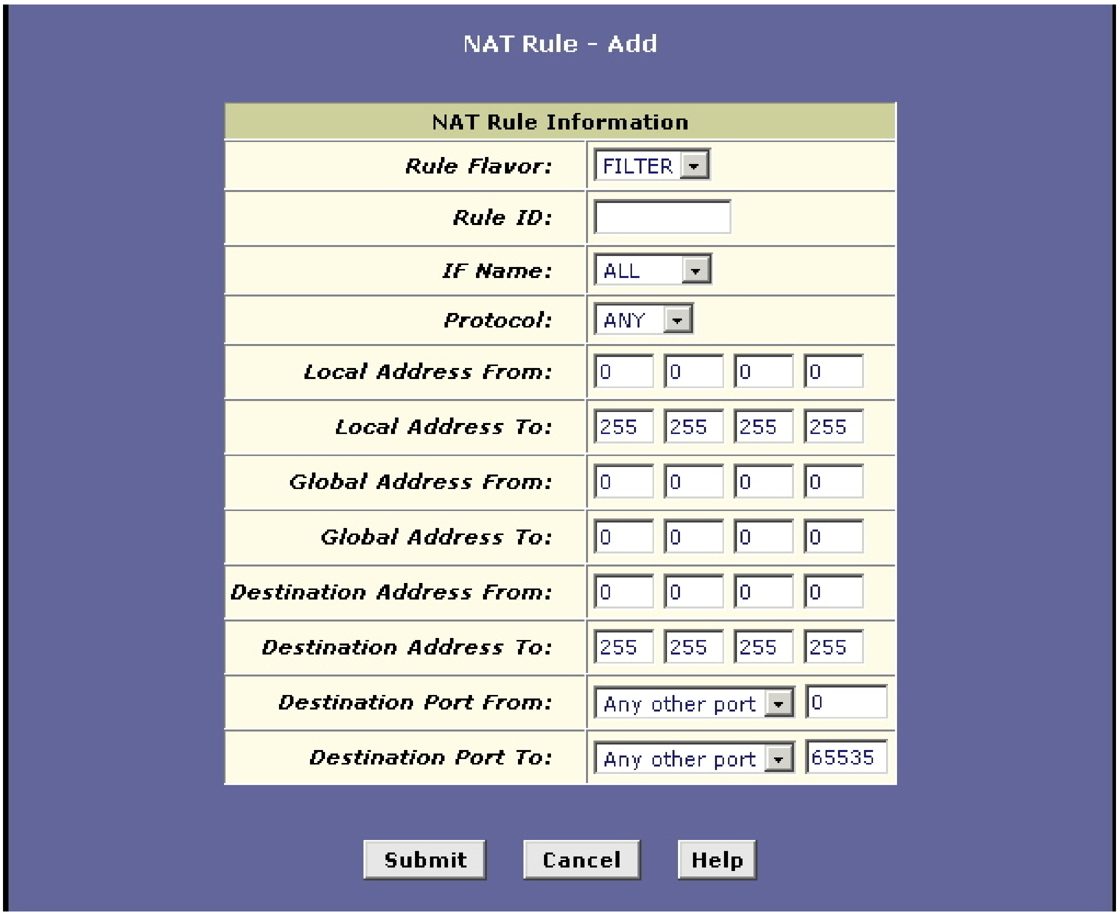
8 On the **NAT Configuration** page, click the **Submit** button. A page appears to confirm your changes.

9 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

8.5.4 The FILTER Rule

Like the BASIC flavor, the FILTER flavor translates public and private IP addresses on a one-to-one basis. The FILTER flavor extends the capability of the BASIC rule.

You can use the FILTER rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, server type (such as FTP or Web server), or both.



NAT Rule - Add

NAT Rule Information				
Rule Flavor:	FILTER			
Rule ID:				
IF Name:	ALL			
Protocol:	ANY			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address From:	0	0	0	0
Global Address To:	0	0	0	0
Destination Address From:	0	0	0	0
Destination Address To:	255	255	255	255
Destination Port From:	Any other port	0		
Destination Port To:	Any other port	65535		

Figure 39: NAT Rule FILTER - Add

1 Display the **NAT Rule - Add** page, select **FILTER** as the Rule Flavor and type a Rule ID.

2 Select the interface and, if desired, a protocol that this rule applies to.

3 In the **Local Address From/To** fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

If you specify a range, each address will be translated in sequency to a corresponding address in a range of global addresses (which you specify in step 4).

4 In the **Global Address From/To** fields, type the starting and ending address that identify the range of public IP addresses to translate your private addresses to. Or, type the same address in both fields (if you also specified a single address in step 3).

5 **Specify a destination port** (or range) if you want this rule to apply to any outbound traffic to the types of servers identified by that port number.

6 When you have completed entering all information, click the **Submit** button. A page appears to confirm the change.

7 Click **Close** to return to the **NAT Configuration** page. The new rule should now be displayed in the NAT Rule table.

8. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected.
9. On the **NAT Configuration** page, click the **Submit** button. A page appears to confirm your changes.
10. Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

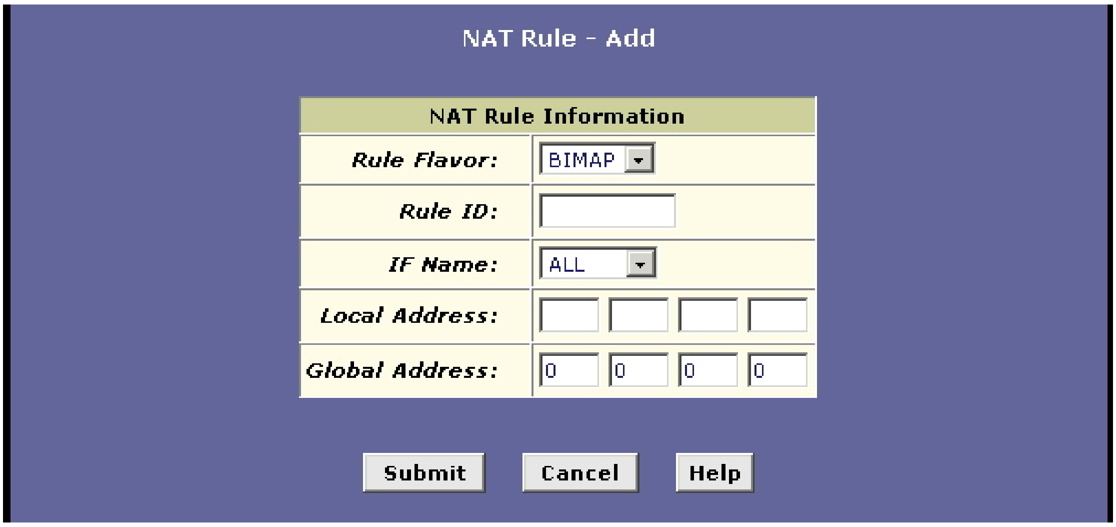
8.5.5 The BIMAP Rule

Unlike the other NAT flavors, the BIMAP flavor performs address translations in both the outgoing and incoming directions.

In the incoming direction, when the specified interface receives a packet destined to your public IP address, this address is translated to the private IP address of a computer on your LAN.

In the outgoing direction, the private source IP address in a data packet is translated to the LAN's public IP address.

BIMAP rules can be used to provide external access to a LAN device. They do not provide the same level of security as RDR rules, because RDR rules also reroute incoming packets based on the port ID. BIMAP rules do not account for the port number, and therefore allow external access regardless of the destination port type specified in the incoming packet.



NAT Rule - Add

NAT Rule Information	
Rule Flavor:	BIMAP
Rule ID:	
IF Name:	ALL
Local Address:	
Global Address:	0 0 0 0

Figure 40: NAT Rule BIMAP - Add

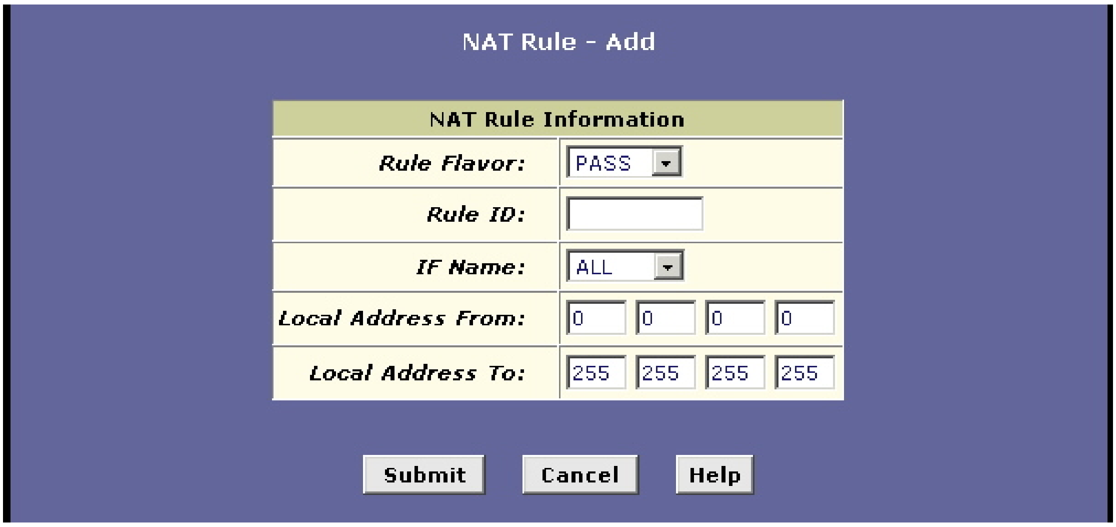
1. Display the **NAT Rule - Add** page, select **BIMAP** as the Rule Flavor and type a Rule ID.
2. Select the interface and, if desired, a protocol that this rule applies to.
3. In the **Local Address** field, type the private IP address of the computer to which you are granting external access.
4. In the **Global Address** field, type the address that you want to serve as the publicly known address for the LAN computer.
5. When you have completed entering all information, click the **Submit** button. A page appears to confirm the change.
6. Click **Close** to return to the **NAT Configuration** page. The new rule should now be displayed in the NAT Rule table.
7. On the **NAT Configuration** page, ensure that the **Enable** radio button is selected.

8 On the **NAT Configuration** page, click the **Submit** button. A page appears to confirm your changes.

9 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

8.5.6 The PASS Rule

You can create a PASS rule to allow a range of IP addresses to remain untranslated when another rule would otherwise do so.



NAT Rule - Add

NAT Rule Information				
Rule Flavor:	PASS			
Rule ID:				
IF Name:	ALL			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255

Figure 41: NAT Rule PASS - Add

The PASS rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. If you want a specific IP address or range of addresses to NOT be subject to an existing rule, say rule ID #5, then you can create a PASS rule with ID #1 through 4.

1 Display the **NAT Rule - Add** page, select **PASS** as the Rule Flavor and type a Rule ID.

2 Select the interface and, if desired, a protocol that this rule applies to.

3 In the **Local Address From/To** fields, type the lowest and highest IP addresses that define the range of private addresses you want to be passed without translation.

If you want the PASS rule to act on only one address, type that address in both fields.

4 When you have completed entering all information, click the **Submit** button. A page appears to confirm the change.

5 Click **Close** to return to the **NAT Configuration** page. The new rule should now be displayed in the NAT Rule table.

6 On the **NAT Configuration** page, ensure that the **Enable** radio button is selected.

7 On the **NAT Configuration** page, click the **Submit** button. A page appears to confirm your changes.

8 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

9 DNS Configuration

This chapter describes how to configure the DNS Relay function on the HM210dp/di.

9.1 DNS Relay Overview

When performing DNS relay, the HM210dp/di itself is not a DNS server, it forwards DNS requests from LAN PCs to a DNS server at the ISP. It then relays the DNS response to the PCs.

The HM210dp/di learns DNS addresses in either or both of the following ways:

- Learned through PPP
- Configured on the HM210dp/di.

9.2 Configuring DNS Relay

Follow these steps to configure DNS relay:

1 Configure the LAN PCs as DHCP clients of the HM210dp/di.

2 Go to **LAN > DHCP Server,** enter the LAN IP address (e.g. **192.168.1.1**) or **0.0.0.0** as the DNS address in the DHCP server pool.

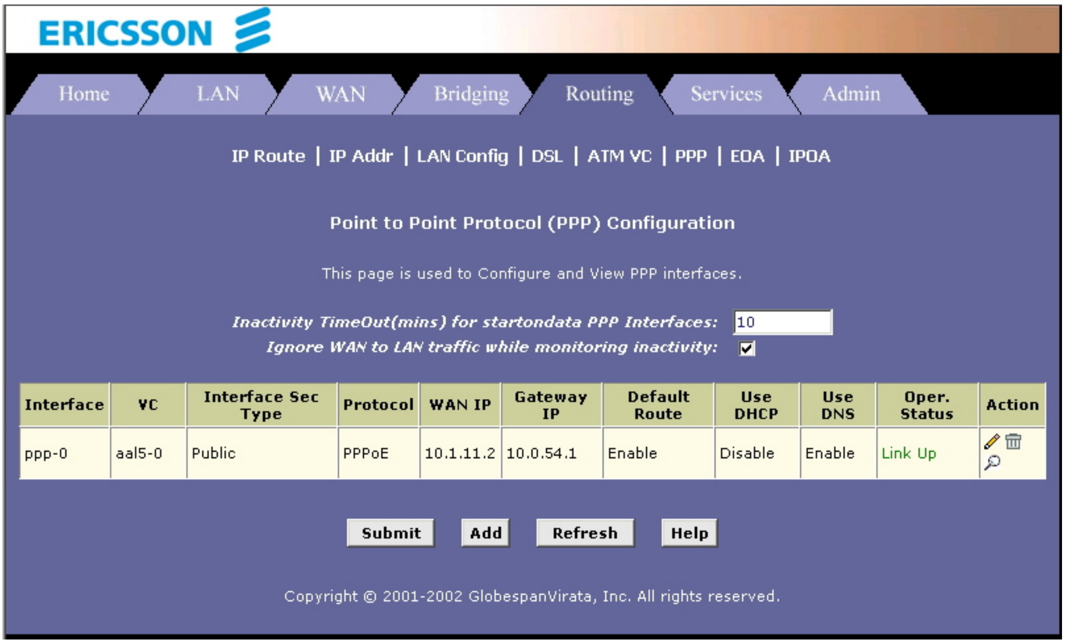
By default, 0.0.0.0 is already set as the DNS of the DHCP pool.

3 Determine how the HM210dp/di will learn the DNS server address:

- **Option 1**: Using a PPP connection to learn the DNS

  Use DNS must be enabled in the PPP interface properties.

  Go to **Routing > PPP** and check the PPP interface details.



Point to Point Protocol (PPP) Configuration

This page is used to Configure and View PPP interfaces.

Inactivity TimeOut(mins) for startondata PPP Interfaces: 10

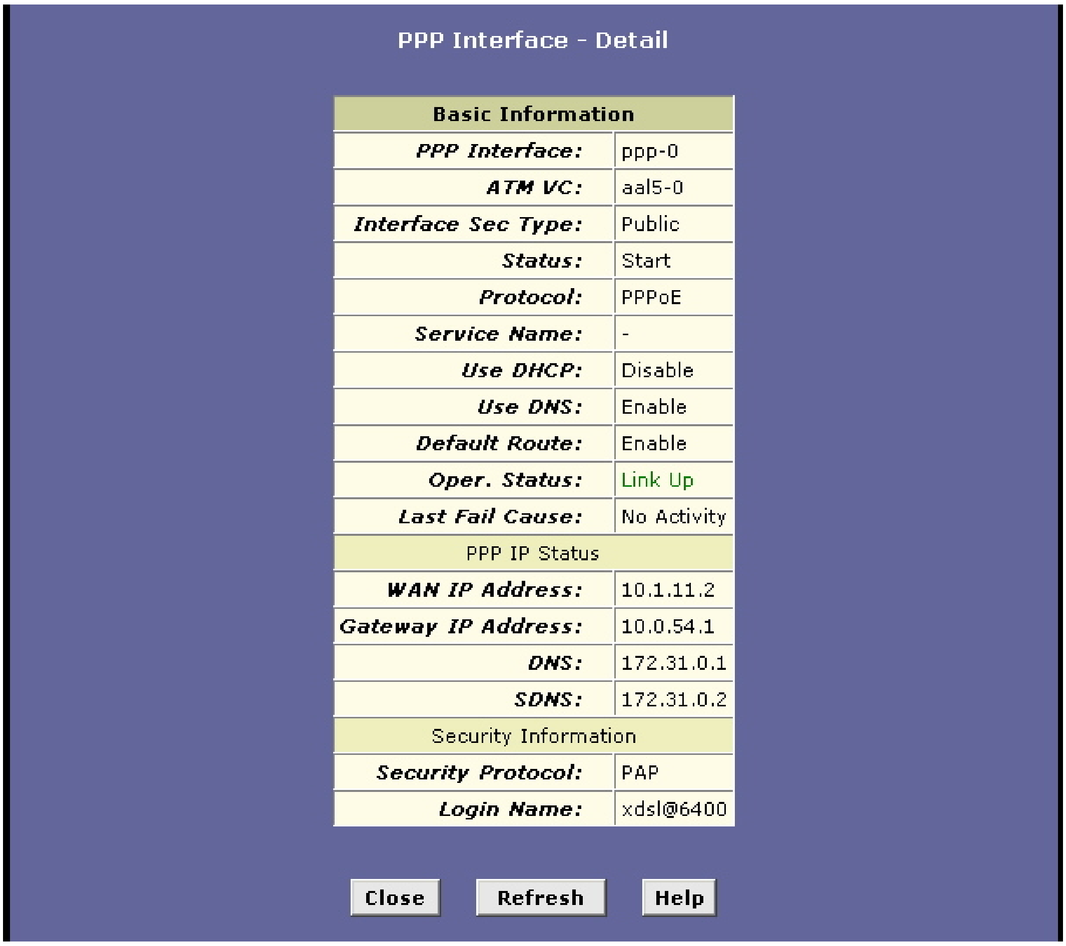
Ignore WAN to LAN traffic while monitoring inactivity: ☑

Interface	VC	Interface Sec Type	Protocol	WAN IP	Gateway IP	Default Route	Use DHCP	Use DNS	Oper. Status	Action
ppp-0	aal5-0	Public	PPPoE	10.1.11.2	10.0.54.1	Enable	Disable	Enable	Link Up	✎ 🗑 🔍

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 42: PPP Configuration

If **Use DNS** is disabled, you must delete the interface and recreate it with the new setting.



PPP Interface - Detail

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
Interface Sec Type:	Public
Status:	Start
Protocol:	PPPoE
Service Name:	-
Use DHCP:	Disable
Use DNS:	Enable
Default Route:	Enable
Oper. Status:	Link Up
Last Fail Cause:	No Activity
PPP IP Status	
WAN IP Address:	10.1.11.2
Gateway IP Address:	10.0.54.1
DNS:	172.31.0.1
SDNS:	172.31.0.2
Security Information	
Security Protocol:	PAP
Login Name:	xdsl@6400

Figure 43: PPP Interface - Detail

- **Option 2**: Configuring DNS on the HM210dp/di:

  You can configure the DNS server address to be relayed on the router if one of the following circumstances applies:

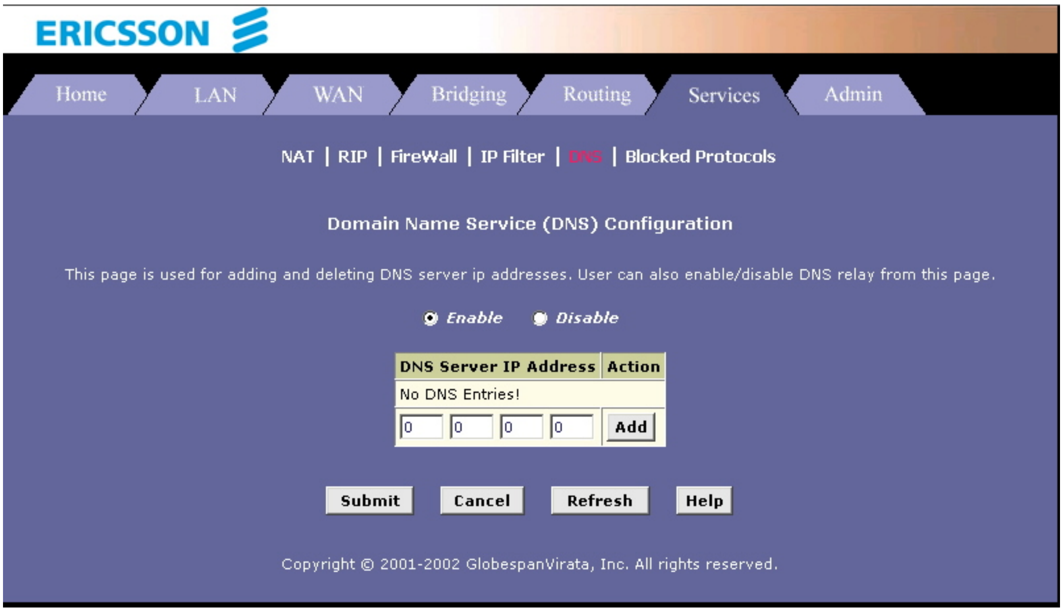
  - Not using PPP connection to the ISP (or a protocol other than PPP is used, such as EoA).

  - You use PPP connection and **Use DNS** is already **enabled**. Then these configured addresses will be used in addition to those DNS addresses learned through PPP.

  - You use PPP connection and **Use DNS** is **disabled**. Then these configured addresses will be used.

  Follow these steps to configure DNS relay on the HM210dp/di:

a Go to **Service** > **DNS** to display the **DNS Configuration** page.



Domain Name Service (DNS) Configuration

This page is used for adding and deleting DNS server ip addresses. User can also enable/disable DNS relay from this page.

● Enable ○ Disable

DNS Server IP Address	Action
No DNS Entries!	
0 0 0 0	Add

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 44: DNS Configuration

b Type the IP address of the DNS server in an empty row and click **Add**. Click the **Enable** radio button, and then click **Submit**.

c Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

10 RIP Configuration

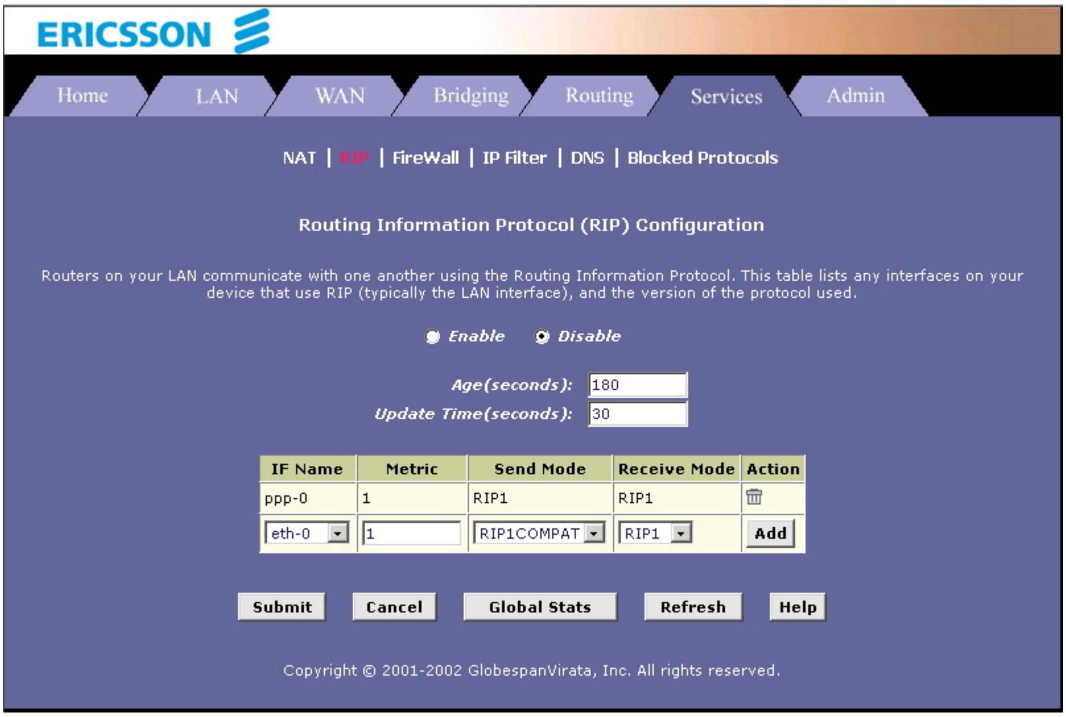
The HM210dp/di can be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. This chapter describes how to configure your HM210dp/di to use one of these, called the Routing Information Protocol (RIP).

Most small home or office networks do not need to use RIP. You may want to configure RIP if any of the following circumstances apply to your network:

- Your network includes an additional router or RIP-enabled PC. The HM210dp/di and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

10.1 Configuring the RIP

1 Select **Services** > **RIP** and the RIP Configuration page appears:



Routing Information Protocol (RIP) Configuration

Routers on your LAN communicate with one another using the Routing Information Protocol. This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used.

○ *Enable* ● *Disable*

Age(seconds): 180

Update Time(seconds): 30

IF Name	Metric	Send Mode	Receive Mode	Action
ppp-0	1	RIP1	RIP1	🗑
eth-0	1	RIP1COMPAT	RIP1	Add

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 45: RIP Configuration

2 If necessary, change the **Age** and **Update** Time. These are global settings for all interfaces that use RIP.

Age Time is the amount of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.

Update Time specifies how frequently the HM210dp/di will send out its routing table to its neighbors.

3 In the **IF Name** column, select the interface on which you want to enable RIP.

For communication with RIP-enabled devices on your LAN, select **eth-0** or the name of the appropriate virtual Ethernet interface.

For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

4 Select a **Metric** value (hop count) for the interface. You can select any integer from 1 to 15.

5 Select a **Send** and **Receive Mode**.

The **Send Mode** setting indicates the RIP version this interface will use when it sends its route information to other devices.

The **Receive Mode** setting indicates the RIP version(s) in which information must be passed to the HM210dp/di in order to it to be accepted into its routing table.

RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.

RIP version 2 is the preferred selection because it supports "classless" IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on the autonomous network support this version of the protocol.

6 Click **Add** in the Action column. The new RIP entry will be displayed in the table.

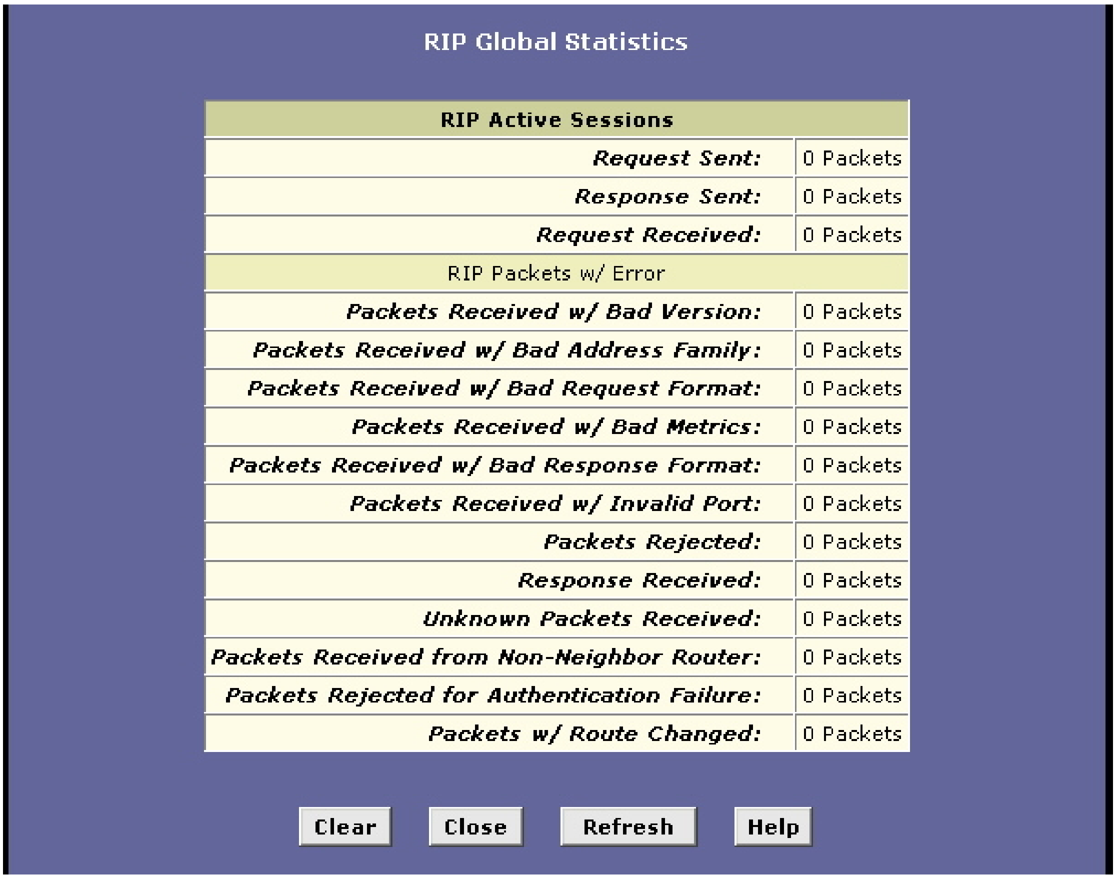
7 Click the **Enable** radio button to enable the RIP feature.

8 When you are finished defining RIP interfaces, click the **Submit** button. A page appears to confirm your changes.

9 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

10.2 Viewing RIP Statistics

To view the RIP statistics, select **Services** > **RIP** > **Global Stats**:



RIP Global Statistics

RIP Active Sessions	
Request Sent:	0 Packets
Response Sent:	0 Packets
Request Received:	0 Packets
RIP Packets w/ Error	
Packets Received w/ Bad Version:	0 Packets
Packets Received w/ Bad Address Family:	0 Packets
Packets Received w/ Bad Request Format:	0 Packets
Packets Received w/ Bad Metrics:	0 Packets
Packets Received w/ Bad Response Format:	0 Packets
Packets Received w/ Invalid Port:	0 Packets
Packets Rejected:	0 Packets
Response Received:	0 Packets
Unknown Packets Received:	0 Packets
Packets Received from Non-Neighbor Router:	0 Packets
Packets Rejected for Authentication Failure:	0 Packets
Packets w/ Route Changed:	0 Packets

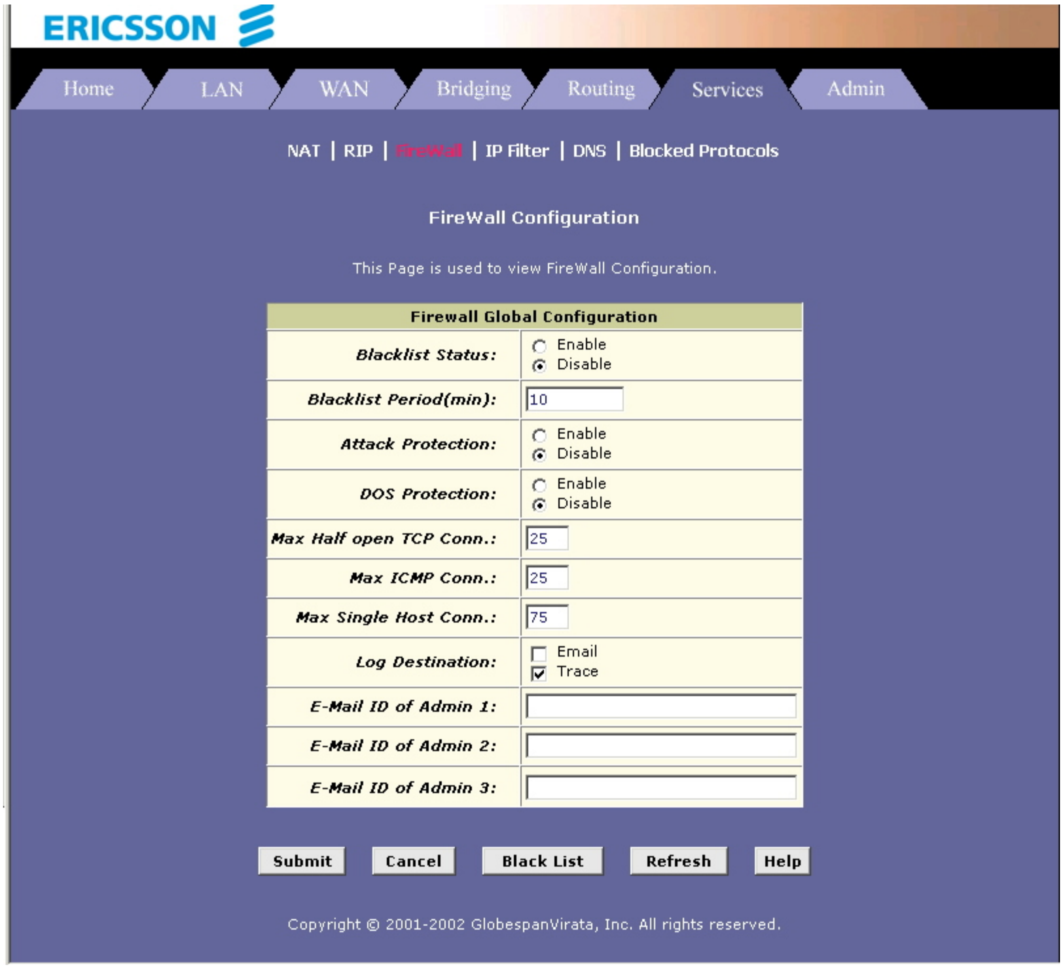
Figure 46: RIP Global Statistics page

11 Firewall Configuration

The Configuration Manager provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

11.1 Global Firewall Settings

1 Select **Services** > **Firewall** and the **Firewall Configuration** page appears:



FireWall Configuration

This Page is used to view FireWall Configuration.

Firewall Global Configuration	
Blacklist Status:	○ Enable ● Disable
Blacklist Period(min):	10
Attack Protection:	○ Enable ● Disable
DOS Protection:	○ Enable ● Disable
Max Half open TCP Conn.:	25
Max ICMP Conn.:	25
Max Single Host Conn.:	75
Log Destination:	□ Email ☑ Trace
E-Mail ID of Admin 1:	
E-Mail ID of Admin 2:	
E-Mail ID of Admin 3:	

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 47: Firewall Configuration

2 Configure any of the following settings:

Field	Description
Blacklist Status	If you want the device to maintain and use a black list, click **Enable**. Click **Disable** if you do not want to maintain a list.
Blacklist Period (min)	Specifies the number of minutes that a computer's IP address will remain on the black list.

Field	Description
Attack Protection	Select **Enable** to use the built-in firewall protections that prevent the following common types of attacks: **IP Spoofing**: Sending packets over the WAN interface using an internal LAN IP address as the source address. **Tear Drop**: Sending packets that contain overlapping fragments. **Smurf and Fraggle**: Sending packets that use the WAN or LAN IP broadcast address as the source address. **Land Attack**: Sending packets that use the same address as the source and destination address. **Ping of Death**: Illegal IP packet length.
DOS Protection	Click the **Enable** radio button to use the following denial of service protections: SYN DoS, ICMP DoS and Per-host DoS protection.
Max Half open TCP Connection	Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
Max ICMP Connection	Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, older ICMP IP sessions will be replaced by new sessions as they are initiated.
Max Single Host Connection	Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.
Log Destination	Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility Ethernet to (Trace) or can be e-mailed to specified administrators.

Field	Description
E-mail ID of Admin 1/2/3	Specifies the e-mail address(es) of the administrator(s) who should receive notices of any attempted firewall violations. Type the address(es) in standard internet e-mail address format, e.g. *jxsmith@onecompany.com* The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number of violations occurring the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

3 Click the **Submit** button.

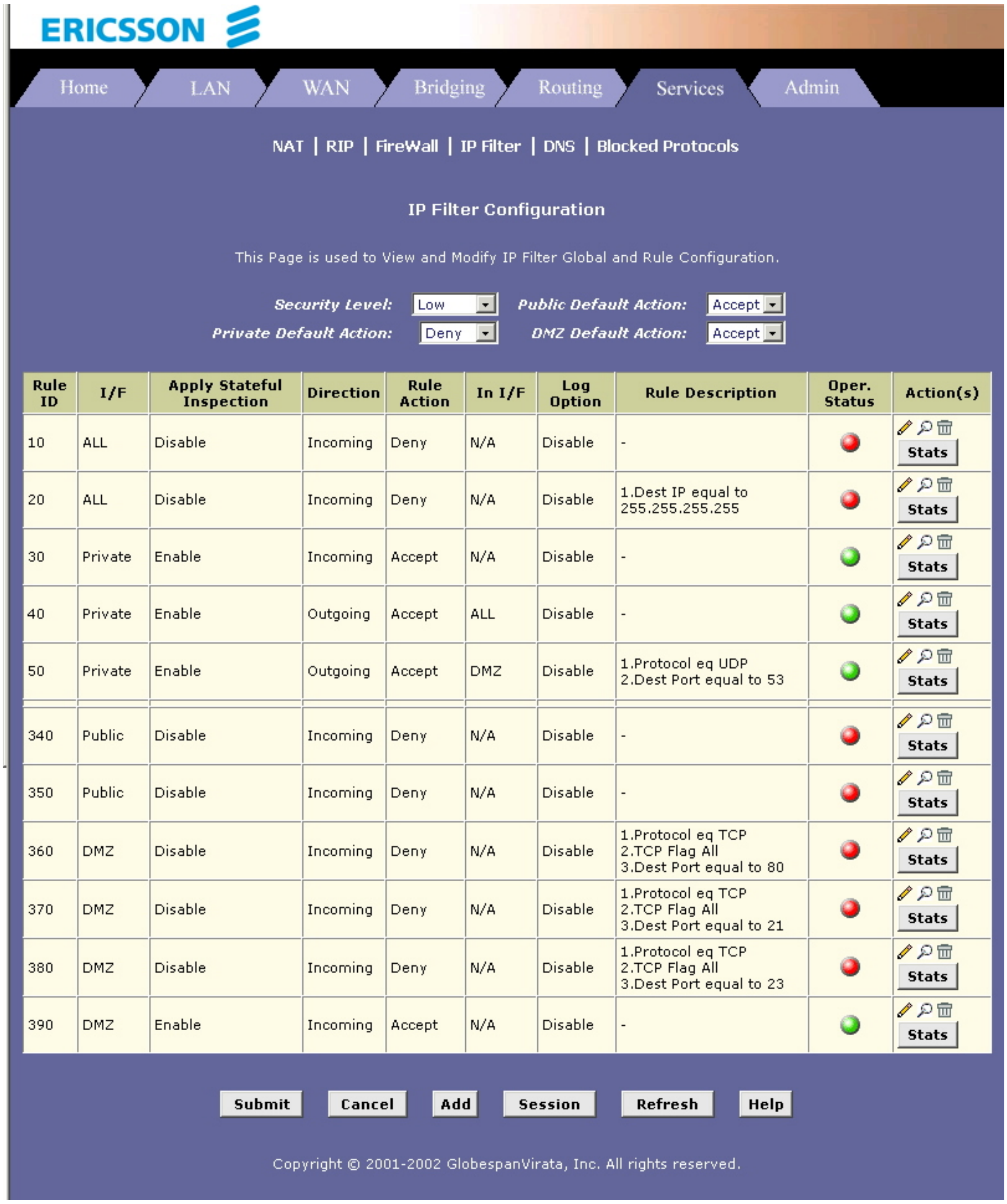
4 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

11.2 IP Filter Configuration

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet.

11.2.1 Viewing Your IP Filter Configuration

Select **Services** > **IP Filter**. The **IP Filter** page appears:



IP Filter Configuration

This Page is used to View and Modify IP Filter Global and Rule Configuration.

Security Level: Low
Public Default Action: Accept
Private Default Action: Deny
DMZ Default Action: Accept

Rule ID	I/F	Apply Stateful Inspection	Direction	Rule Action	In I/F	Log Option	Rule Description	Oper. Status	Action(s)
10	ALL	Disable	Incoming	Deny	N/A	Disable	-	🔴	Stats
20	ALL	Disable	Incoming	Deny	N/A	Disable	1.Dest IP equal to 255.255.255.255	🔴	Stats
30	Private	Enable	Incoming	Accept	N/A	Disable	-	🟢	Stats
40	Private	Enable	Outgoing	Accept	ALL	Disable	-	🟢	Stats
50	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq UDP 2.Dest Port equal to 53	🟢	Stats
340	Public	Disable	Incoming	Deny	N/A	Disable	-	🔴	Stats
350	Public	Disable	Incoming	Deny	N/A	Disable	-	🔴	Stats
360	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 80	🔴	Stats
370	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 21	🔴	Stats
380	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 23	🔴	Stats
390	DMZ	Enable	Incoming	Accept	N/A	Disable	-	🟢	Stats

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 48: IP Filter Configuration page

11.2.2 Configuring IP Filter Global Settings

The **IP Filter Configuration** page enables you to configure several global IP Filter settings, and displays a table showing all existing IP Filter rules. The global settings that you can configure are:

- **Security Level**: When **High** is selected, only those rules that are assigned a security value of High will be in effect. The same is true for the **Medium** and **Low** settings. When **None** is selected, IP Filtering is disabled.
- **Private/Public/DMZ Default Action**: This setting specifies a default action to be taken (**Accept** or **Deny**) on private, public, or DMZ-type device interfaces when they receive packets that **do not** match any of the filtering rules.

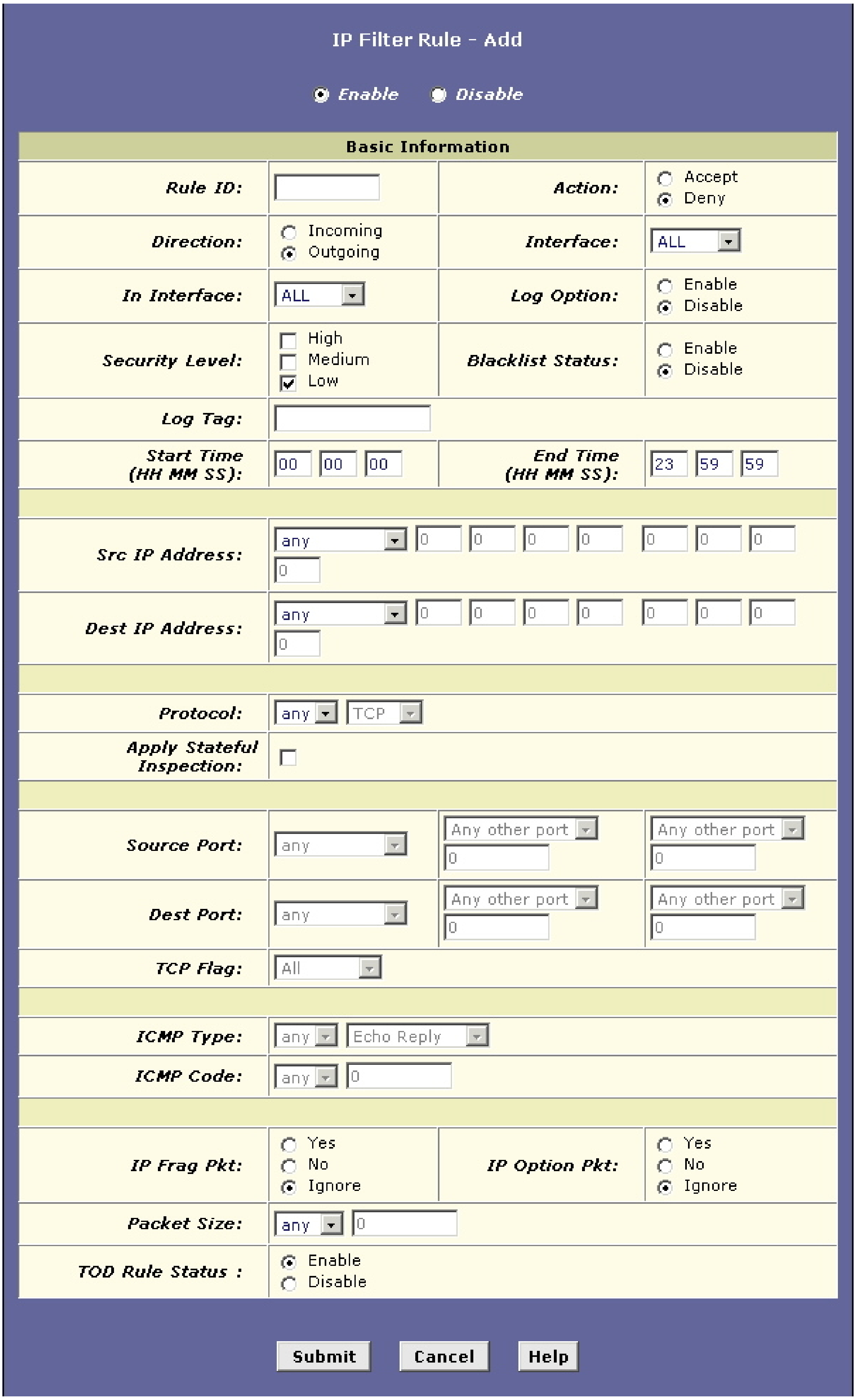
  Public - The interface connect to the Internet, e.g. PPP, EoA and IPoA interfaces. Typically, the global setting for public interfaces is **Deny**, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP Filter rule.

  Private - Typically, the global setting for private interfaces is **Accept**, so that LAN computers have access to the Internet connection of the HM210dp/di.

  DMZ - Refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface - whether from a LAN or external source - are subject to a set of protections that is in between public and private interfaces. The global setting for DMZ-type interfaces may be set to **Deny** so that all attempts to access these servers are denied by default. The administrator may then configure IP Filter rules to allow accesses of certain types.

11.2.3 Creating IP Filter Rules

1 On the main **IP Filter** page, click **Add**. The **IP Filter Rule - Add** page appears:



IP Filter Rule - Add

● Enable ○ Disable

Basic Information

Rule ID:		Action:	○ Accept ● Deny
Direction:	○ Incoming ● Outgoing	Interface:	ALL
In Interface:	ALL	Log Option:	○ Enable ● Disable
Security Level:	□ High □ Medium ☑ Low	Blacklist Status:	○ Enable ● Disable
Log Tag:			
Start Time (HH MM SS):	00 00 00	End Time (HH MM SS):	23 59 59
Src IP Address:	any 0 0 0 0 0 0 0 0 0		
Dest IP Address:	any 0 0 0 0 0 0 0 0 0		
Protocol:	any TCP		
Apply Stateful Inspection:	□		
Source Port:	any	Any other port 0	Any other port 0
Dest Port:	any	Any other port 0	Any other port 0
TCP Flag:	All		
ICMP Type:	any Echo Reply		
ICMP Code:	any 0		
IP Frag Pkt:	○ Yes ○ No ● Ignore	IP Option Pkt:	○ Yes ○ No ● Ignore
Packet Size:	any 0		
TOD Rule Status :	● Enable ○ Disable		

Figure 49: IP Filter Rule - Add

2 Enter or select data for each field that applies to your rule:

Field	Description
Rule ID	Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g. 10, 20, 30) so that you leave enough space between them for inserting a new rule if necessary.
Action	The action can be **Accept** (forward to destination) or **Deny** (discard the packet).
Direction	**Incoming** refers to packets coming from the LAN, and **outgoing** refers to packets going to the Internet.
Interface	The interface on which the rule will take affect.
In Interface	The interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only for the outgoing direction.
Log Option	When **Enable** is selected, a log entry will be created on the system each time this rule is invoked.
Security Level	The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to Medium and the global firewall level is set to Medium, then the rule will be active; but if the global firewall level is set to High or Low, then the rule will be inactive.
Blacklist Status	Specifies whether or not a violation of this rule will result in the offending computer's IP address being added to the Black List, which blocks the router from forwarding packets from that source for a specified period of time.
Log Tag	A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to **Enable** if you configure a Log Tag.
Start/End Time	The time range during which this rule is to be in effect, specified in military units.

Field	Description
Src IP Address	IP address critera for the source computer(s) from which the packet originates. Use the following expressions to specify IP: **any**: any source IP address **lt**: less than **lteq**: less than or equal to **gt**: greater than **eq**: equal to **neq**: not equal to **range**: within the specified range, inclusive **out of range**: outside the specified range **self**: the IP address of the router interface on which this rule takes effect.
Dest IP Address	IP address rule criteria for the destination computer(s), i.e. the IP address of the computer to which the packet is being sent. In addition to the options described for the Src IP Address field, the following option is available: **bcast**: Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface). When you select this option, you do not need to specify the address, so the address fields are dimmed.
Protocol	The basic IP protocol criteria that must be met for a rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (eq), that they must not contain the specified protocol (neq), or that the rule can be invoked regardless of the protocol (any). TCP, UDP and ICMP are commonly IP protocols; others can be identified by number from 0-255 as defined by IANA.
Apply Stateful Inspection	If this option is enabled, then **stateful filtering** is performed and the rule is also applied in the other direction on the given interface during an IP session.
Source Port	Port number criteria for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) if you have not specified a protocol critera. See the description of Src IP Address for the selection options.
Dest Port	Port number criteria for the destination computer(s), i.e. the port number of the type of computer to which the packet is being sent. This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.

Field	Description
TCP Flag	Specifies whether the rule should apply only to TCP packets that contain the synchronous (SYN) flag, only to those that contain the non-synchronous (NOT-SYN) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.
ICMP Type	Specifies whether the value in the type field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0 to 255. You can specify that the value must be equal (eq) or not equal (neq) to the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
ICMP Code	Specifies whether the value in the code field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0 to 255. You can specify that the value must be equal (eq) or not equal (neq) to the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
IP Frag Pkt	Determines how the rule applies to IP packets that contain fragments. You can choose from the following options: **Yes**: The rule will be applied only to packets that contain fragments. **No**: The rule will be applied only to packets that do not contain fragments. **Ignore**: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.
IP Option Pkt	Determines whether the rule should apply to IP packets that have options specified in their packet headers. You can choose from the following options: **Yes**: The rule will be applied only to packets that contain header options. **No**: The rule will be applied only to packets that do not contain header options. **Ignore**: (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.
Packet Size	Specifies that the IP Filter rule will take affect only on packets whose size in bytes matches this criteria. (lt=less than, gt=greater than, lteq=less than or equal to, etc).

Field	Description
TOD Rule Status	The Time of Day Rule Status determines how the Start Time/End Time settings are used. **Enable**: (Default) The rule is in effect for the specified time period. **Disable**: The rule is not in effect for the specified time period, but is effective at all other times.

3 When you are done selecting criteria, ensure that the **Enable** radio button is selected and then click the **Submit** button.

If the security level of the rule matches the globally configured setting, a green ball in the Status column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different than the globally configured level.

4 Ensure that the **Security Level** and **Private/Public/DMZ Default Action** settings on the **IP Filter Configuration** page are configured as needed, then click **Submit**.

5 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

11.2.3.1 IP Filter Rule Examples

Example 1 - Blocking a specific computer on your LAN from accessing web servers on the Internet:

1 Add a new rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0 interface, for eaxmple).

2 Specify a source IP address of the computer you want to block.

3 Specify the Protocol = TCP and enable the Store State setting.

4 Specify a destination port = 80, which is the standard port number for web servers.

5 Enable the rule by clicking the radio button at the top of the page.

6 Click **Submit** to create the rule.

7 On the **IP Filter Configuration** page, set the **Security Level** to the same level you chose for the rule, and set both the **Private Default Action** and the **Public Default Action** to **Accept**.

8 Click **Submit** and commit your changes.

Example 2 - Blocking Telnet access to the device:

1 Add a new rule for incoming packets on the ppp-0 interface.

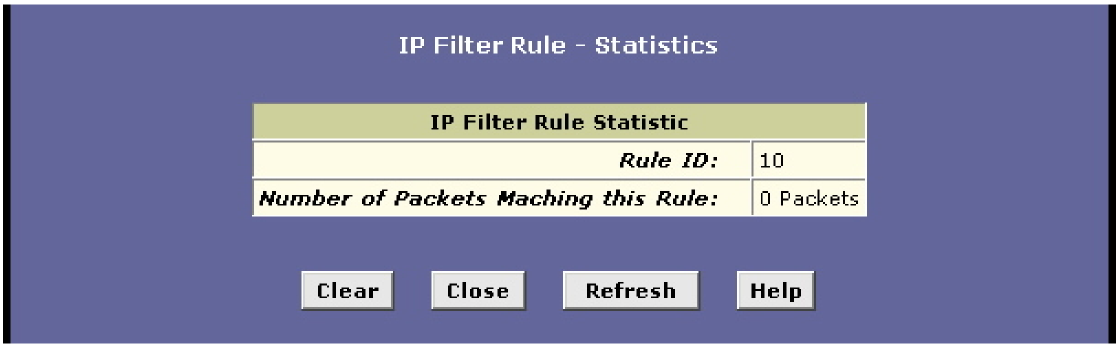
2 Specify that the packet must contain the TCP protocol, and must be destined for port 23, the standard port number used for the Telnet protocol.

3 Enable the rule by clicking the radio button at the top of the page.

4 Click **Submit** to create the rule, and commit your changes.

11.2.4 Viewing IP Filter Statistics

To view statistics on how many packets were accepted or denied for a rule, select **Services** > **IP Filter** > **Stats** in the row corresponding to the rule:



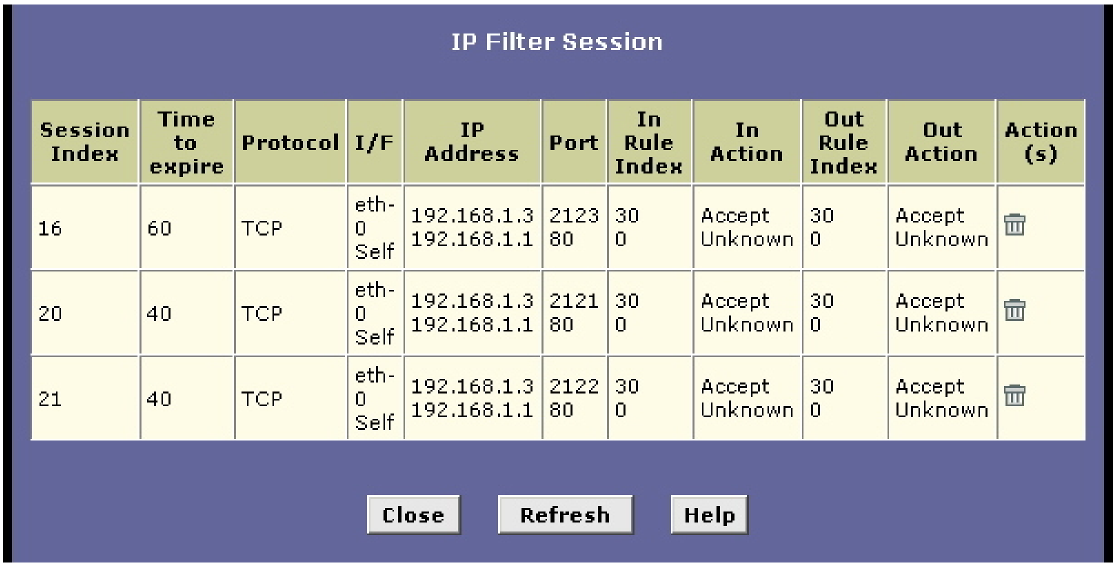
IP Filter Rule - Statistics

IP Filter Rule Statistic	
Rule ID:	10
Number of Packets Maching this Rule:	0 Packets

Figure 50: IP Filter Rule - Statistics

11.2.5 Managing Current IP Filter Sessions

To view all current IP session, select **Services** > **IP Filter** > **Session** to display the **IP Filters Session** page:



IP Filter Session

Session Index	Time to expire	Protocol	I/F	IP Address	Port	In Rule Index	In Action	Out Rule Index	Out Action	Action (s)
16	60	TCP	eth-0 Self	192.168.1.3 192.168.1.1	2123 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑
20	40	TCP	eth-0 Self	192.168.1.3 192.168.1.1	2121 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑
21	40	TCP	eth-0 Self	192.168.1.3 192.168.1.1	2122 80	30 0	Accept Unknown	30 0	Accept Unknown	🗑

Figure 51: IP Filter Session

The IP Filter Session table displays the following fields:

Field	Description
Session Index	The ID assigned by the system to the IP session (all sessions, whether or not they are affected by an IP filter rule, are assigned a session index).
Time to expire	The number of seconds in which the connection will automatically expire.
Protocol	The underlying IP protocol used on the connection, such as TCP, UDP, IGMP, etc.).
I/F	The interface on which the IP Filter rule is effective.

Field	Description
IP Address	The IP addresses involved in the communication. The first one shown is the initiator of the communication.
Port	The hardware addresses of the ports involved in the commmunication.
In/Out Rule Index	The number of the IP Filter rule that is applied to this session (assigned when the rule was created).
In/Out Action	The action (accept, deny, or unknown) being taken on data coming in to or going out from the interface. This action is specified in the rule definition.

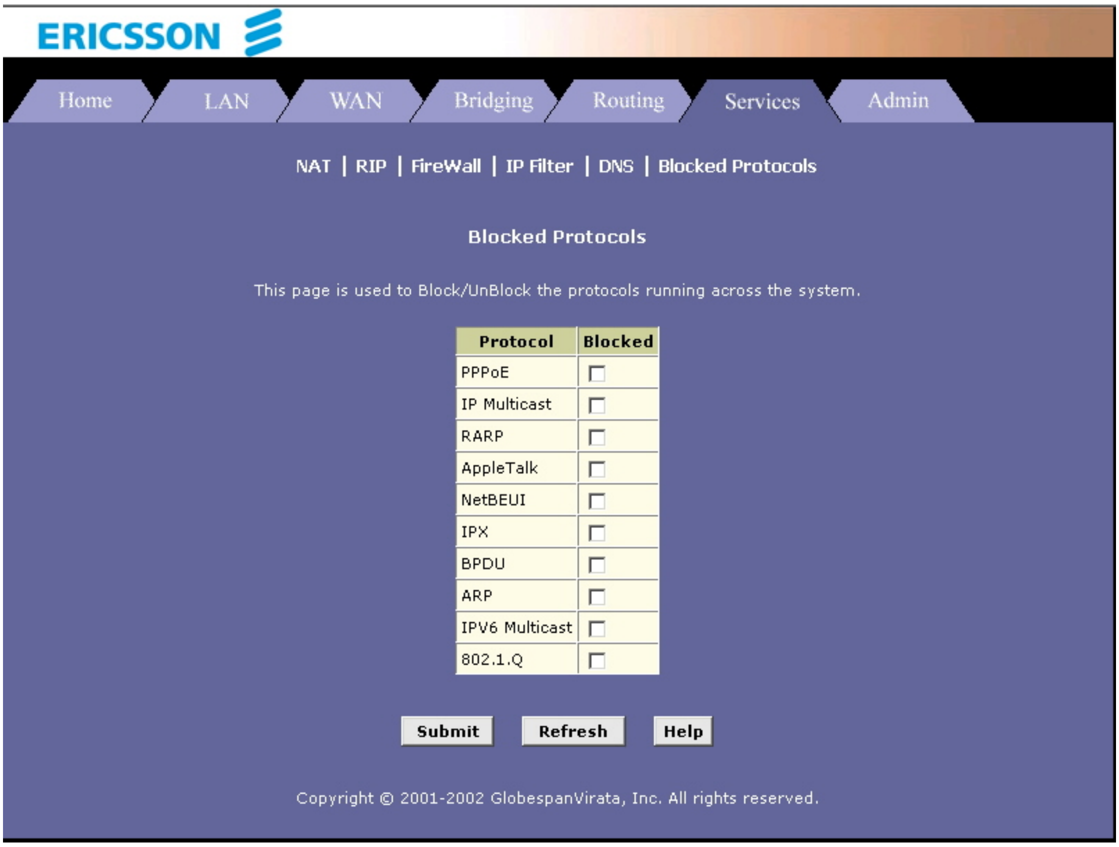
11.3 To Block Specific Protocols

The Blocked Protocols feature prevents the HM210dp/di from passing any data that uses a particular protocol. Unlike the IP Filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations.

Note:

Blocking certain protocols may disrupt or disable your network communication or Internet access. DO NOT use this feature unless you are certain that a particular protocol is not needed or wanted on your network.

To block specific protocols running across the system, select **Services** > **Blocked Protocols**.



Blocked Protocols

This page is used to Block/UnBlock the protocols running across the system.

Protocol	Blocked
PPPoE	□
IP Multicast	□
RARP	□
AppleTalk	□
NetBEUI	□
IPX	□
BPDU	□
ARP	□
IPV6 Multicast	□
802.1.Q	□

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 52: Blocked Protocols

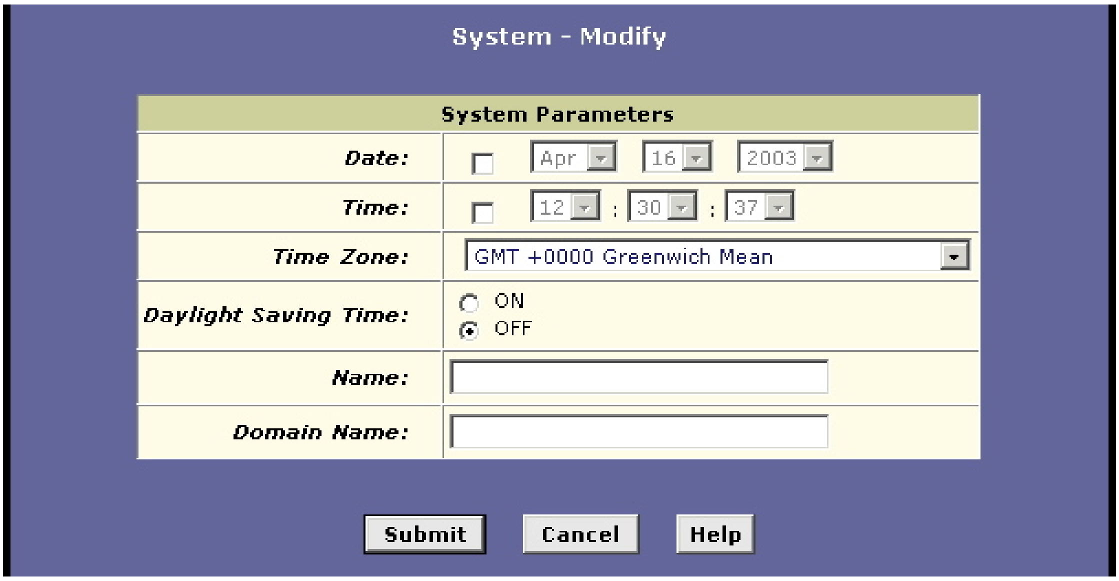
Check the protocol type you want to block and click the **Submit** button. Make sure to use the Commit feature to save your changes to the permanent memory.

To unblock a specific protocol, uncheck the protocol and repeat the submit and commit tasks.

12 Administration Tasks

12.1 Changing the System Date and Time

The HM210dp/di keeps a record of the current date and time, which it uses to calculate and report various performance data. You can select **Home > Modify** to change the date and time as required. You may also specify the host name and the domain name in the fields provided.



System - Modify

System Parameters

Date:	□ Apr 16 2003
Time:	□ 12 : 30 : 37
Time Zone:	GMT +0000 Greenwich Mean
Daylight Saving Time:	○ ON ● OFF
Name:	
Domain Name:	

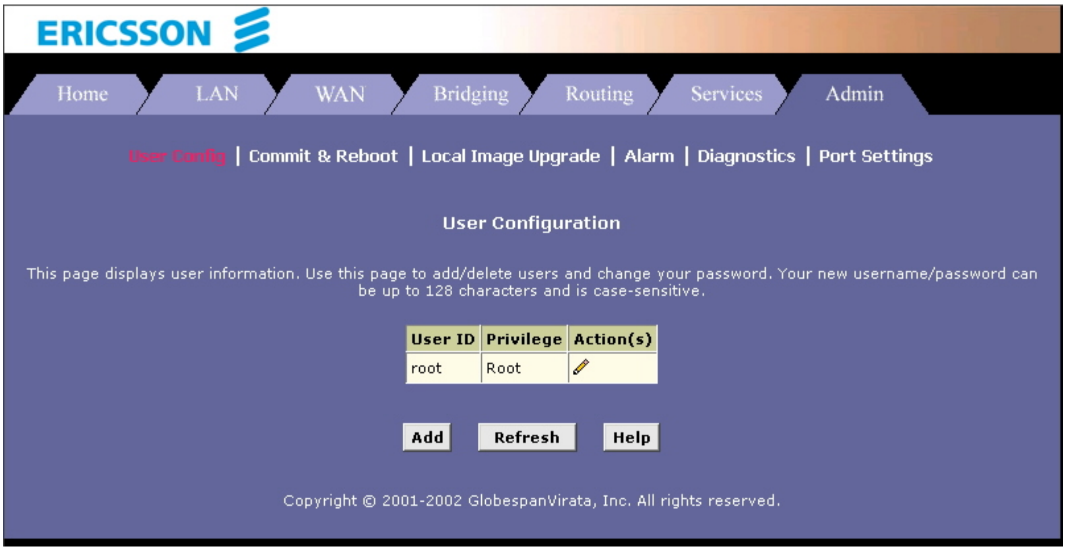
Figure 53: System - Modify

12.2 Adding Login User ID and Changing Login Password

The first time you log into the Configuration Manager, you use the default User ID and Password (root and root). The system allows two levels of privilege: **Root** and **User**. Root privilege allows you to change and commit the device's settings while user privilege is provided with read-only access rights.

To add login User ID or change login password:

1 Select **Admin** > **User Config**. The **User Configuration** page appears:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Add
Refresh
Help

User Configuration

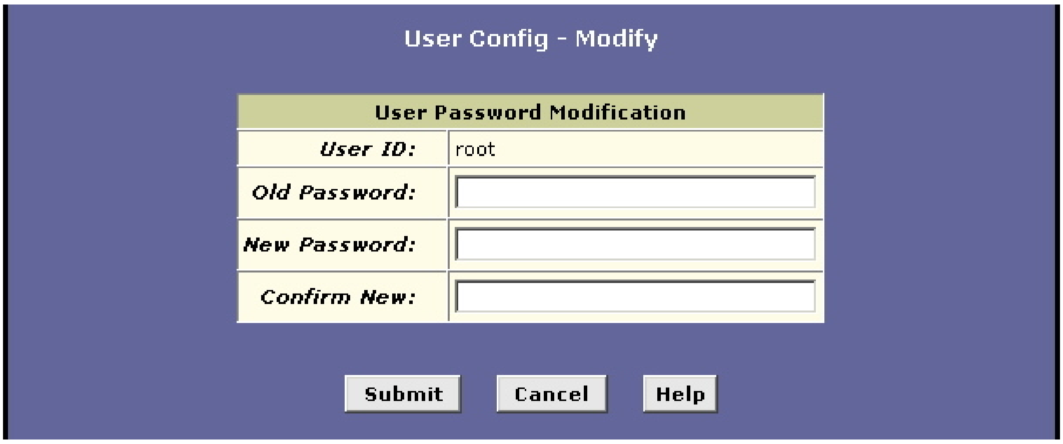
This page displays user information. Use this page to add/delete users and change your password. Your new username/password can be up to 128 characters and is case-sensitive.

User ID	Privilege	Action(s)
root	Root	✎

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 54: User Configuration page

2 To modify the login password, click the **modify** icon in the Action(s) column and then change the current password:



User Config - Modify

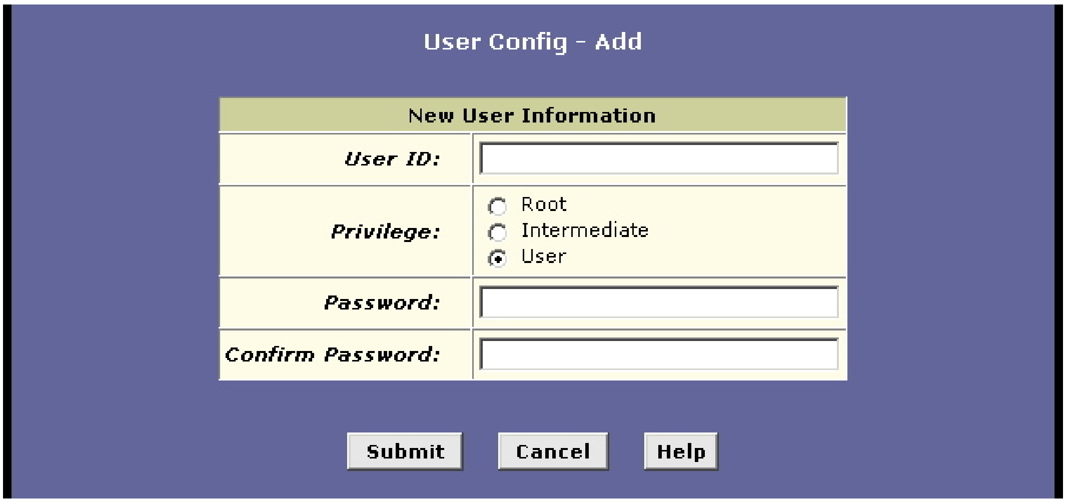
User Password Modification	
User ID:	root
Old Password:	
New Password:	
Confirm New:	

Figure 55: Change Password

3 To add a new login ID, click **Add** to display the **User Config - Add** page. Enter your settings in the fields provided.

Note:

Both the User ID and Password are case sensitive.



User Config - Add

New User Information

User ID:	
Privilege:	○ Root ○ Intermediate ● User
Password:	
Confirm Password:	

Figure 56: User Config - Add

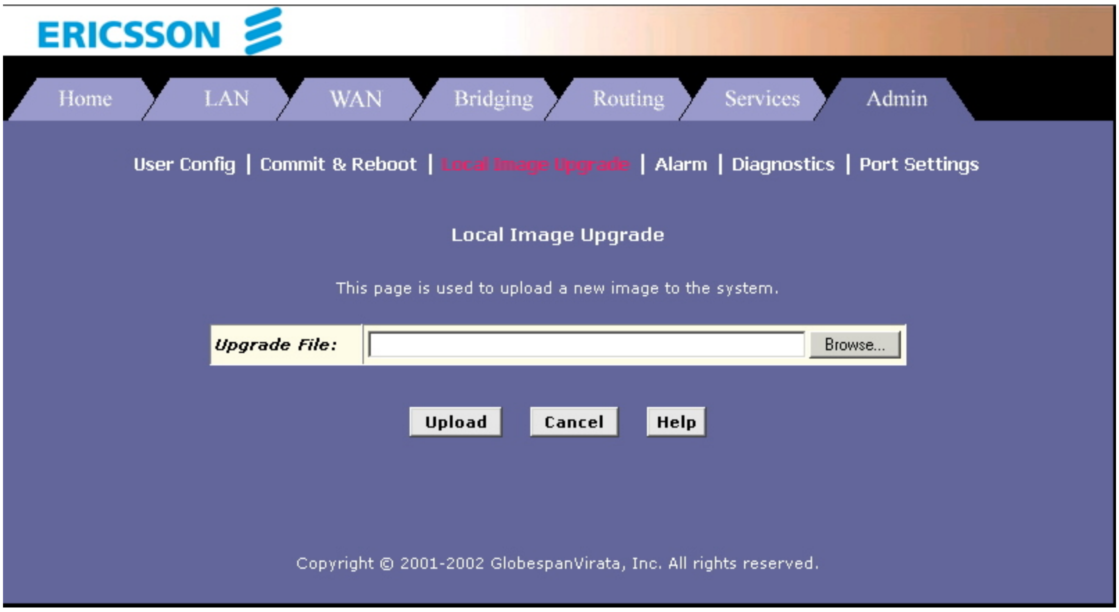
4 After making changes, click the **Submit** button.

5 Select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

12.3 Image Upgrade

This option allows you to upgrade the HM210dp/di to new firmware. After upgrading, your customized configuration will still exist and not be reset to the factory defaults. To perform the upgrade task, download the required firmware file to your host PC and follow the steps below:

Select **Admin** > **Local Image Upgrade** to view the Local Image Upgrade page:



ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings

Local Image Upgrade

This page is used to upload a new image to the system.

Upgrade File:	

Browse...
Upload
Cancel
Help

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 57: Local Image Upgrade page

1 Click **Browse** to locate the firmware file.

The name of the upgrade file must be one of the following:

TEImage.bin, TEDsl.gsz, TEAppl.gsz, Filesys.bin, TEPatch.bin

2 Click **Upload** to start the upgrade. After a few seconds, a message like the following should appear (the file name may differ):

```
File: TEDsl.gsz successfully saved to the flash. Please
reboot for the new image to take effect.
```

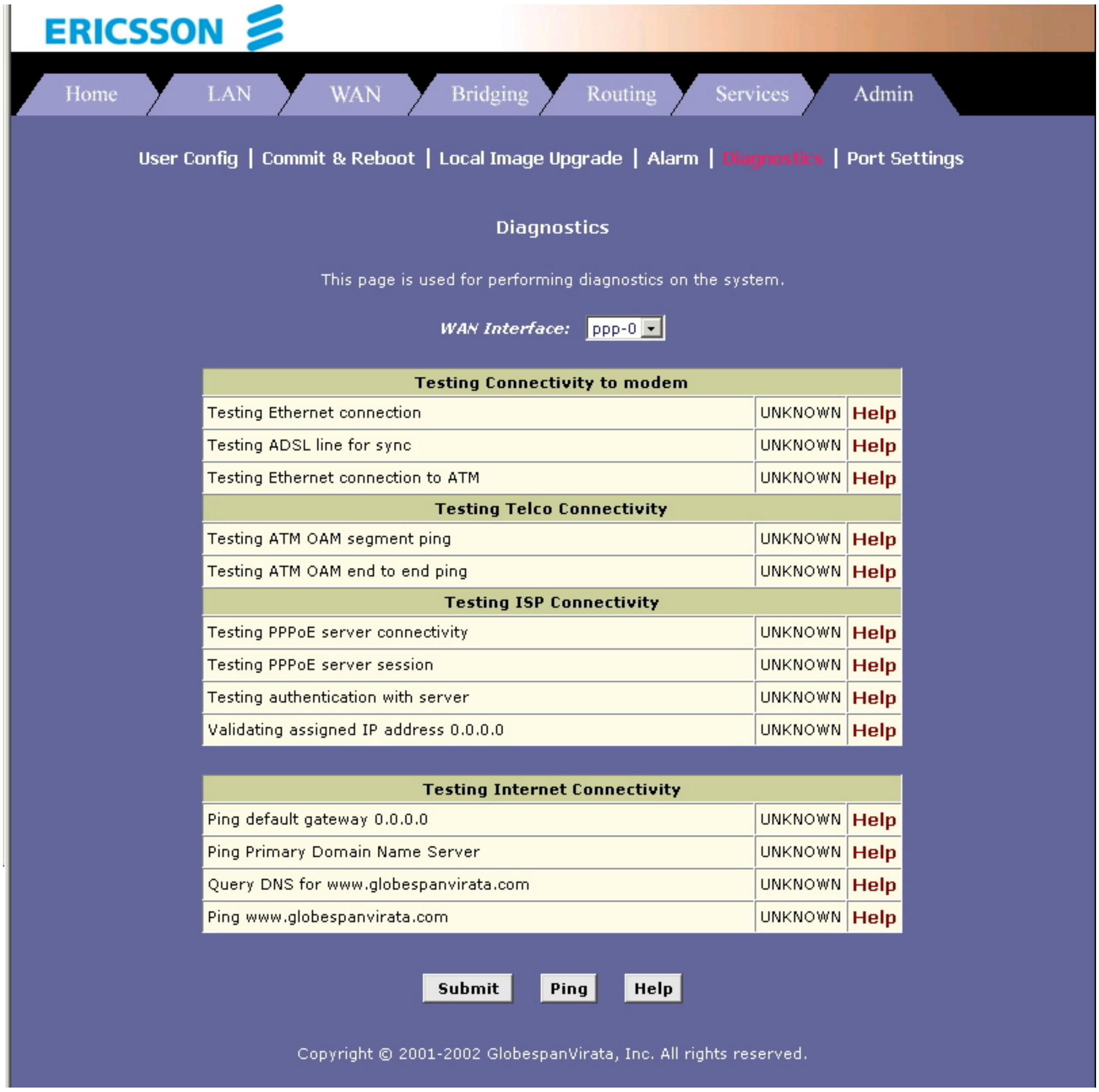
3 Power off the unit, wait a few seconds, and then turn it on again to activate the new software.

Note:

Do not interrupt the upgrade process. Otherwise it might cause damage to your router.

12.4 Diagnostics

To perform diagnostics on ATM VC, select **Admin** > **Diagnostics**. Select the VC on which you want to execute diagnostics and then click **Submit**. The diagnostic result will be displayed. Note that only the VCs defined in the system will appear in the drop-down list.


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Submit
Ping
Help

Diagnostics

This page is used for performing diagnostics on the system.

WAN Interface: ppp-0

Testing Connectivity to modem		
Testing Ethernet connection	UNKNOWN	Help
Testing ADSL line for sync	UNKNOWN	Help
Testing Ethernet connection to ATM	UNKNOWN	Help
Testing Telco Connectivity		
Testing ATM OAM segment ping	UNKNOWN	Help
Testing ATM OAM end to end ping	UNKNOWN	Help
Testing ISP Connectivity		
Testing PPPoE server connectivity	UNKNOWN	Help
Testing PPPoE server session	UNKNOWN	Help
Testing authentication with server	UNKNOWN	Help
Validating assigned IP address 0.0.0.0	UNKNOWN	Help

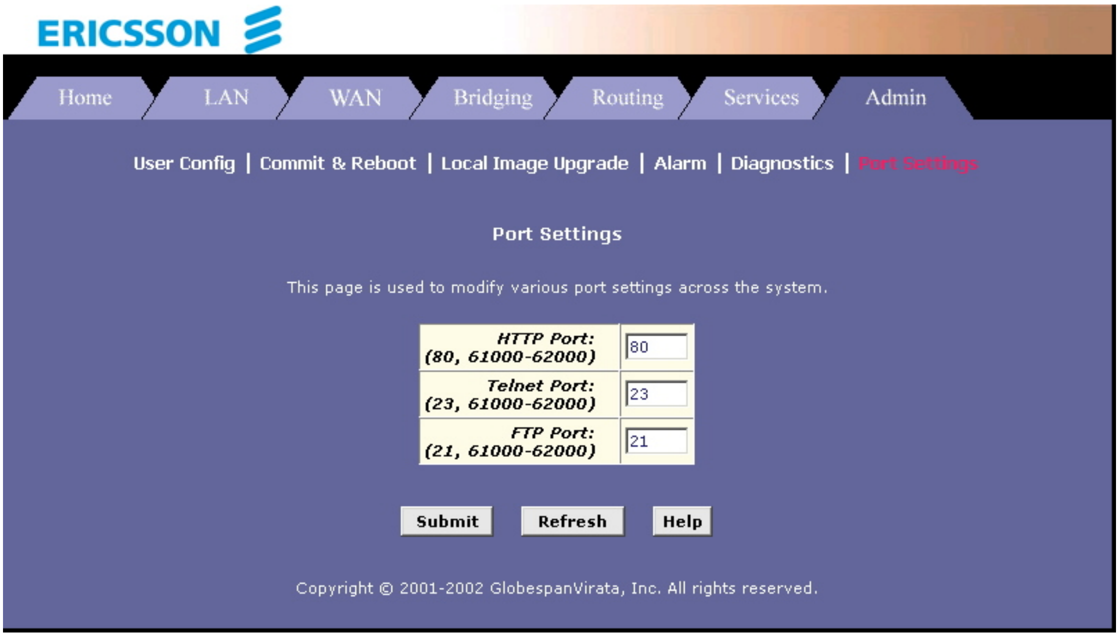
Testing Internet Connectivity		
Ping default gateway 0.0.0.0	UNKNOWN	Help
Ping Primary Domain Name Server	UNKNOWN	Help
Query DNS for www.globespanvirata.com	UNKNOWN	Help
Ping www.globespanvirata.com	UNKNOWN	Help

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 58: Diagnostics page

12.5 Port Settings

The router's HTTP/Telnet/FTP service are accessible using the standard port number 80, 23 and 21 respectively. It is possible that you want to designate a publicly accessible HTTP, Telnet or FTP server on your LAN side and you want to shift the router's HTTP/Telnet/FTP service to use a non-standard port number. If this is the case, select **Admin** > **Port Settings** to view the **Port Settings** page:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Submit
Refresh
Help

Port Settings

This page is used to modify various port settings across the system.

HTTP Port: (80, 61000-62000)	80
Telnet Port: (23, 61000-62000)	23
FTP Port: (21, 61000-62000)	21

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 59: Port Settings page

Modify the port settings and click the **Submit** button. Then select **Admin** > **Commit & Reboot** and click **Commit** to save your changes to permanent storage.

Note:

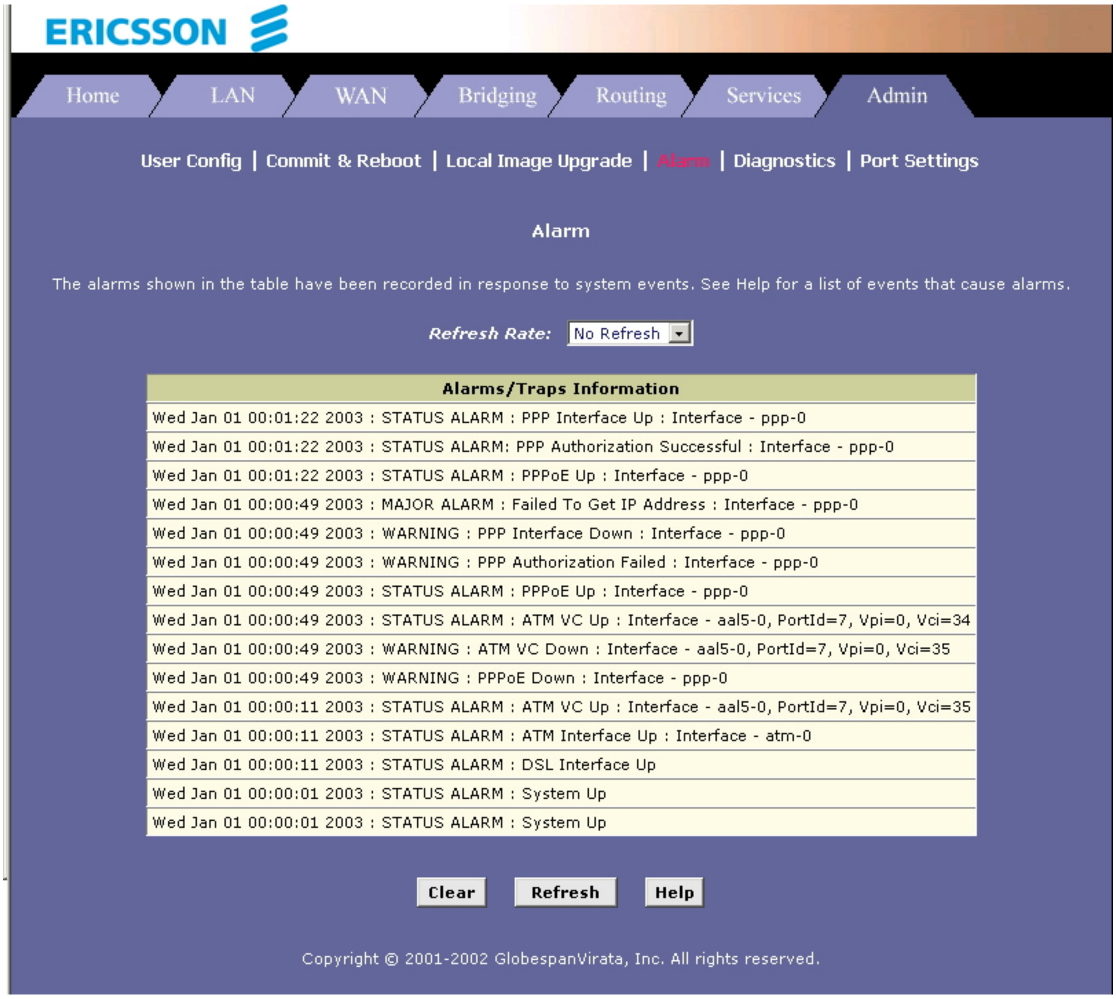
If you set the router's embedded HTTP/Telnet/FTP server to use a non-standard port number, when access from the external world, the IP address should be followed by a colon and the non-standard port number, as shown in the following example for a HTTP server (i.e. the Web-based Configuration Manager):

```
http://10.0.1.16:61000
```

where **10.0.1.16** is the router's WAN IP address and **61000** is the non-standard port number for HTTP that you specified in the Port Settings page.

12.6 View System Alarms

To display the alarm page select **Admin** > **Alarm**:


ERICSSON
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Alarm | Diagnostics | Port Settings
Clear
Refresh
Help

Alarm

The alarms shown in the table have been recorded in response to system events. See Help for a list of events that cause alarms.

Refresh Rate: No Refresh

Alarms/Traps Information
Wed Jan 01 00:01:22 2003 : STATUS ALARM : PPP Interface Up : Interface - ppp-0
Wed Jan 01 00:01:22 2003 : STATUS ALARM: PPP Authorization Successful : Interface - ppp-0
Wed Jan 01 00:01:22 2003 : STATUS ALARM : PPPoE Up : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : MAJOR ALARM : Failed To Get IP Address : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : WARNING : PPP Interface Down : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : WARNING : PPP Authorization Failed : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : STATUS ALARM : PPPoE Up : Interface - ppp-0
Wed Jan 01 00:00:49 2003 : STATUS ALARM : ATM VC Up : Interface - aal5-0, PortId=7, Vpi=0, Vci=34
Wed Jan 01 00:00:49 2003 : WARNING : ATM VC Down : Interface - aal5-0, PortId=7, Vpi=0, Vci=35
Wed Jan 01 00:00:49 2003 : WARNING : PPPoE Down : Interface - ppp-0
Wed Jan 01 00:00:11 2003 : STATUS ALARM : ATM VC Up : Interface - aal5-0, PortId=7, Vpi=0, Vci=35
Wed Jan 01 00:00:11 2003 : STATUS ALARM : ATM Interface Up : Interface - atm-0
Wed Jan 01 00:00:11 2003 : STATUS ALARM : DSL Interface Up
Wed Jan 01 00:00:01 2003 : STATUS ALARM : System Up
Wed Jan 01 00:00:01 2003 : STATUS ALARM : System Up

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

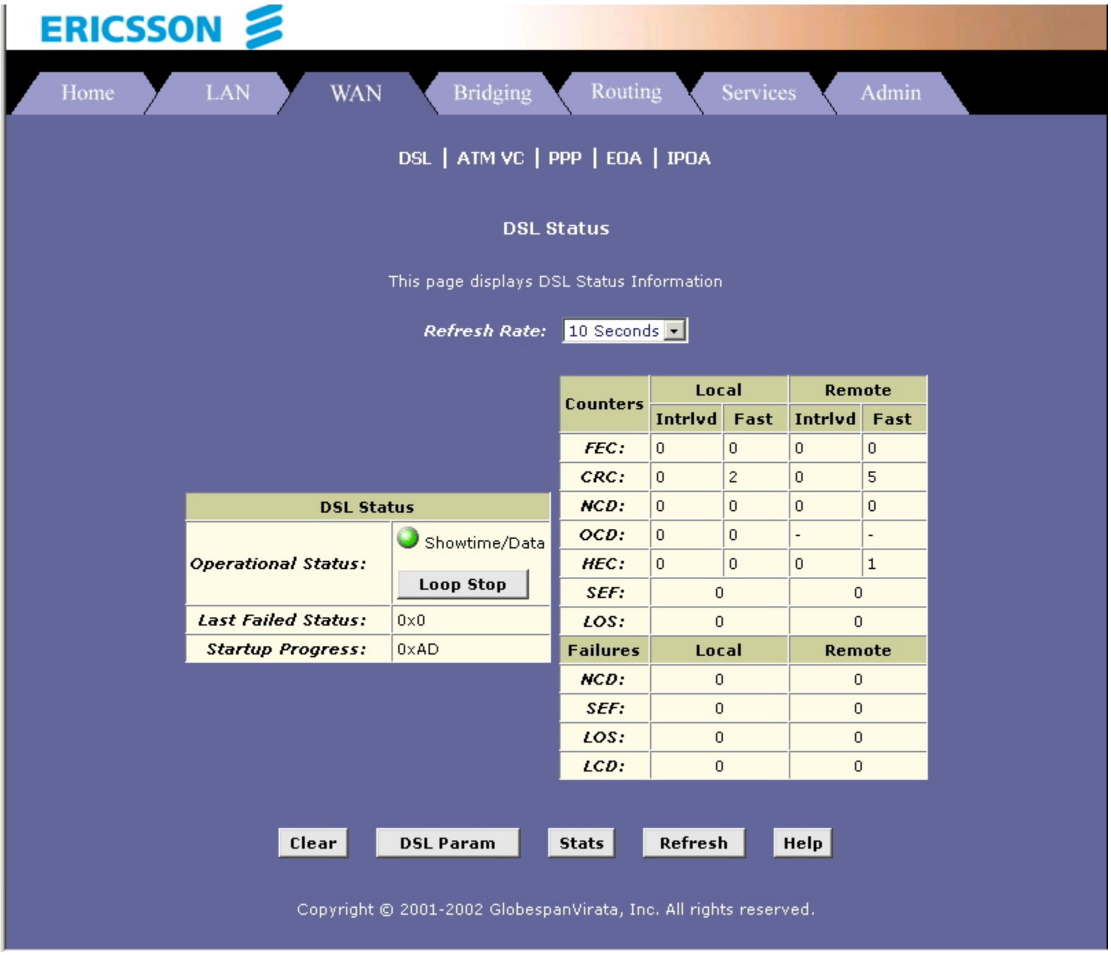
Figure 60: Alarm page

Each row in the table displays the time and date when an alarm occurred, the type of alarm, and a brief statement indicating its cause.

You can click on the **Refresh Rate** drop-down list to select a recurring time interval after which the page will be redisplayed with new data.

13 View DSL Parameters

To view configuration parameters and performance statistics for the ADSL line, select **WAN** > **DSL**. The **DSL Status** page displays:



DSL Status

This page displays DSL Status Information

Refresh Rate: 10 Seconds

DSL Status	
Operational Status:	● Showtime/Data Loop Stop
Last Failed Status:	0x0
Startup Progress:	0xAD

Counters	Local		Remote	
	Intrlvd	Fast	Intrlvd	Fast
FEC:	0	0	0	0
CRC:	0	2	0	5
NCD:	0	0	0	0
OCD:	0	0	-	-
HEC:	0	0	0	1
SEF:	0		0	
LOS:	0		0	

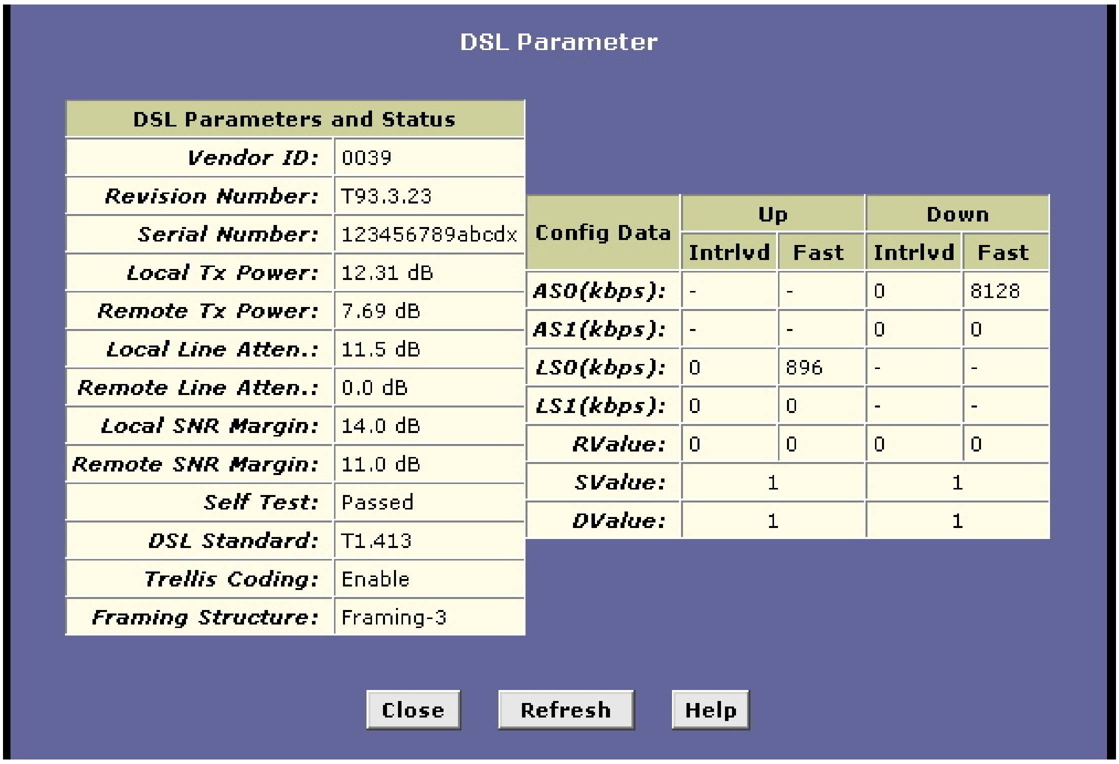
Failures	Local	Remote
NCD:	0	0
SEF:	0	0
LOS:	0	0
LCD:	0	0

Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

Figure 61: DSL Status page

The **DSL Status** page displays the current information on the DSL line performance. The page refreshes about every 10 seconds.

You can click **DSL Param** to display data about the configuration of the DSL line, as shown below:



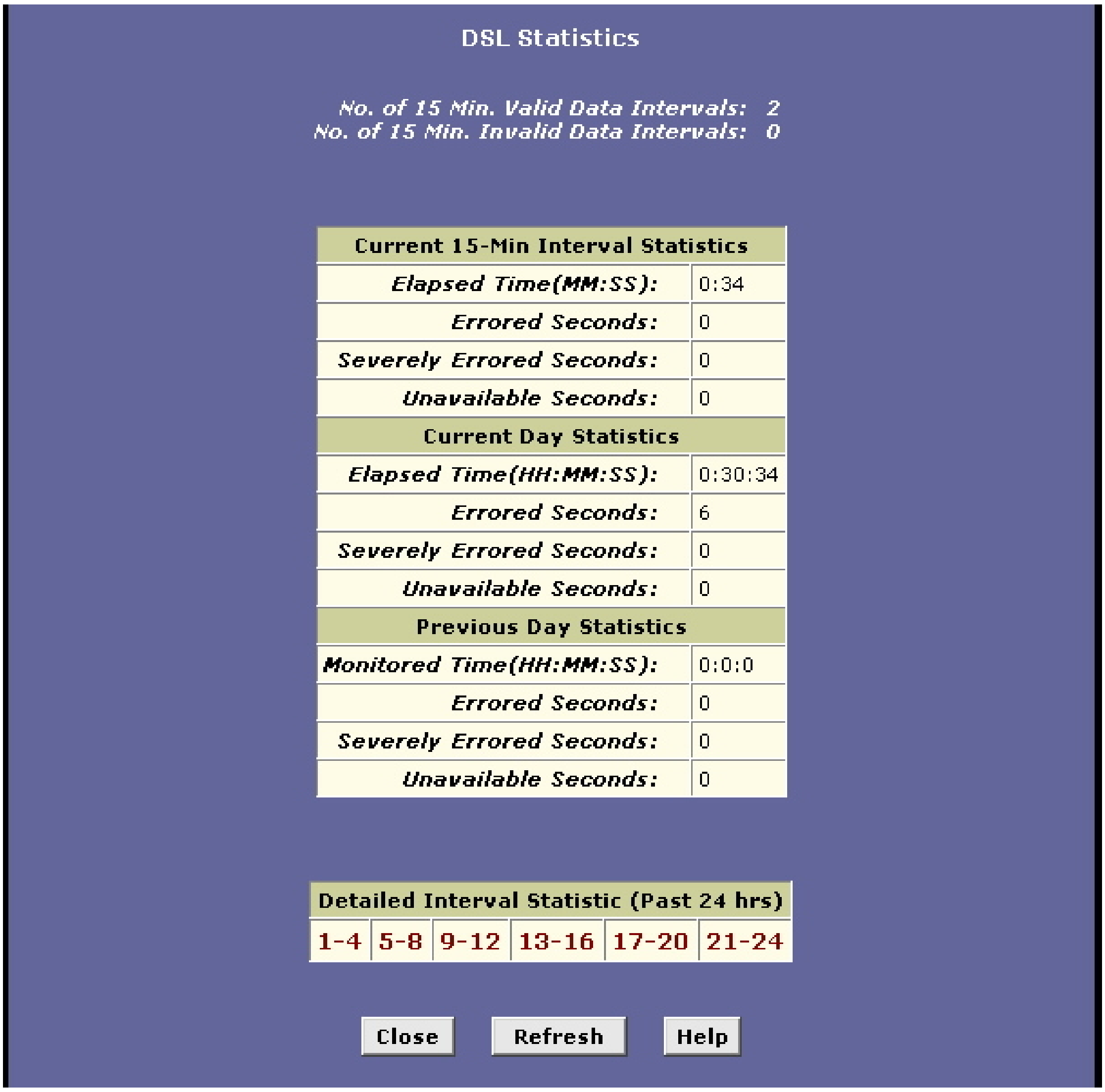
DSL Parameter

DSL Parameters and Status	
Vendor ID:	0039
Revision Number:	T93.3.23
Serial Number:	123456789abcdx
Local Tx Power:	12.31 dB
Remote Tx Power:	7.69 dB
Local Line Atten.:	11.5 dB
Remote Line Atten.:	0.0 dB
Local SNR Margin:	14.0 dB
Remote SNR Margin:	11.0 dB
Self Test:	Passed
DSL Standard:	T1.413
Trellis Coding:	Enable
Framing Structure:	Framing-3

Config Data	Up		Down	
	Intrlvd	Fast	Intrlvd	Fast
AS0(kbps):	-	-	0	8128
AS1(kbps):	-	-	0	0
LS0(kbps):	0	896	-	-
LS1(kbps):	0	0	-	-
RValue:	0	0	0	0
SValue:	1		1	
DValue:	1		1	

Figure 62: DSL Parameter

From the **DSL Status** page you can click **Stats** to display DSL line performance statistics:



DSL Statistics

No. of 15 Min. Valid Data Intervals: 2
No. of 15 Min. Invalid Data Intervals: 0

Current 15-Min Interval Statistics	
Elapsed Time(MM:SS):	0:34
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0
Current Day Statistics	
Elapsed Time(HH:MM:SS):	0:30:34
Errored Seconds:	6
Severely Errored Seconds:	0
Unavailable Seconds:	0
Previous Day Statistics	
Monitored Time(HH:MM:SS):	0:0:0
Errored Seconds:	0
Severely Errored Seconds:	0
Unavailable Seconds:	0

Detailed Interval Statistic (Past 24 hrs)					
1-4	5-8	9-12	13-16	17-20	21-24

Figure 63: DSL Statistics

The **DSL Statistics** page reports error data relating to the last 15 mintues interval, the current day, and the previous day.

At the bottom of the page, the **Detailed Interval Statistics** table displays links you can click to display detailed data for each 15 minute interval in the past 24 hours. For example, when you click on 1-4, data displays for the 15-minute such intervals that make up the prevous 4 hours (there are 16 of these) shows one such page.

14 Troubleshooting

This chapter suggests solutions for problems you may encounter when installing or using your HM210dp/di, and provides instructions for using several IP utilities to diagnose problems.

14.1 LEDs

Problem	Troubleshooting Suggestion
The PWR LED does not illuminate after product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connted to the HM210dp/di and a wall socket/power strip.
The DSL LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable is securely connected to the DSL port and your wall phone jack. Wait 30 seconds to allow the device to negotiate a connection with your ISP.
The LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the HM210dp/di. Make sure the PC and/or hub is turned on. Verify that you are using the correct cable. See "Connecting the Hardware" for more information.
The DIAG LED stays illuminated after turning the device on.	The DIAG LED should turn off after about 10-15 seconds. If it does not, turn of the HM210dp/di, wait 10 seconds, and then turn it back on.

14.2 Internet Access

Problem	Troubleshooting Suggestion
PC cannot access the Internet	Use the PING utility to check whether your PC can communicate with the LAN IP address (by default 192.168.1.1) of the HM210dp/di. If it cannot, check the Ethernet cabling. If you have assigned a static IP address to the computer (not a registered public address), verify the following: Check that the gateway IP address on the computer is your public IP address. If it is not, correct the address or configure the PC to receive IP information automatically. Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically. Verify that a NAT rule has been defined on the HM210dp/di to translate the private address to your public IP address.
PCs cannot display web pages on the Internet	Verify that the DNS server specified on the PCs is correct for your ISP. You can use the PING utility to test connectivity with your ISP's DNS server.

14.3 Configuration Manager Program

Problem	Troubleshooting Suggestion
You forgot/lost your Configuration Manager user ID and/or Password.	You can reset the HM210dp/di to the default configuration by pressing the Reset button for 3 times on the back panel of the device (using a pointed object such as a paper clip). **WARNING!** Resetting the HM210dp/di removes any custom settings and returns all settings to their default values.
Cannot access the Configuration Manager program from your browser	Use the PING utility to check whether your PC can communicate with the LAN IP address (by default 192.168.1.1) of the HM210dp/di. If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer v5.0 or later, or Netscape Navigator v5.0 or later. Support for Javascript® must be enabled in your browser. Support for Java® may also be required. Verify that the PCs IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the HM210dp/di.
Changes to the Configuration Manager program are not being retained.	Make sure to use the **Commit & Reboot** function after making any changes.

15 Important Information

15.1 Product Care and Maintenance

Note:

These are important guidelines for safe and efficient use of your device. Read this information before using your Ericsson ADSL Modem HM210dp/di.

Your ADSL Modem HM210dp/di is a highly sophisticated electronic device. To get the most out of your product, be sure to read the following text about product care, safety and efficient use.

Do not expose the product to liquid or moisture.

Do not expose the product to extreme temperatures, neither hot nor cold.

Do not expose the product to lit candles, cigarettes, cigars, open flames, etc.

Do not drop, throw or try to bend the product. Rough treatment may damage the product.

Do not attempt to disassemble your product. The warranty is no longer valid if the warranty seal has been broken. The product does not contain consumer serviceable components. Service should only be performed by Certified Service Centres.

Do not allow children to play with the product as it contains small parts that could be detached and create a choking hazard.

Avoid using this telephone equipment during an electrical storm. There may be a remote risk of electric shock from lightning.

Use only original Ericsson components and replacement parts. Failure to do so may result in performance loss, damage to the product, fire, electric shock or injury; and will invalidate the warranty.

Use only the power supply adapter that comes with the unit. Replacement power supply adapters can be obtained from Ericsson upon request.

Treat the product with care, keep it in an clean and dust free place. Use only a soft, damp cloth to clean the product.

15.2 Regulatory Information

15.2.1 EU Directives

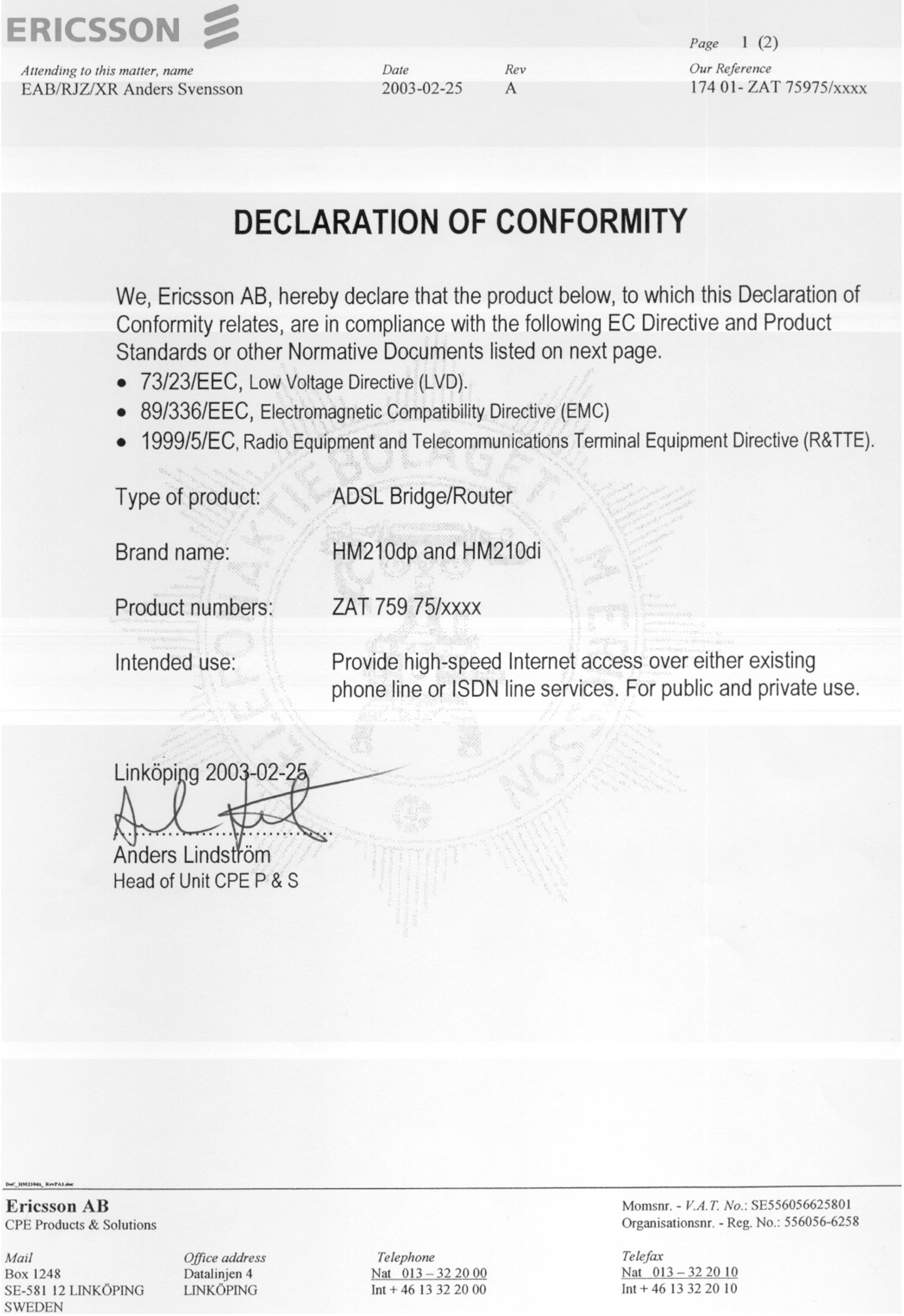
The HM210dp/di meet the following EU directives for the CE mark:

- 73/23/EEC, Low Voltage Directive (LVD)
- 89/336/EEC, Electromagnetic Compatibility Directive (EMC)
- 1999/5/EC, Radio Equipment and Telecommunication Terminal Directive (R&TTE).

15.2.1.1 CE Requirement

Hereby, Ericsson AB, declares that this ADSL Modem HM210dp/di is in conformity with the essential requirements and other relevant provisions of the R&TTE directive 1999/5/EC.

15.2.1.2 Declaration of Conformity



ERICSSON

Page 1 (2)

Attending to this matter, name	Date	Rev	Our Reference
EAB/RJZ/XR Anders Svensson	2003-02-25	A	174 01- ZAT 75975/xxxx

DECLARATION OF CONFORMITY

We, Ericsson AB, hereby declare that the product below, to which this Declaration of Conformity relates, are in compliance with the following EC Directive and Product Standards or other Normative Documents listed on next page.

- 73/23/EEC, Low Voltage Directive (LVD).
- 89/336/EEC, Electromagnetic Compatibility Directive (EMC)
- 1999/5/EC, Radio Equipment and Telecommunications Terminal Equipment Directive (R&TTE).

Type of product:	ADSL Bridge/Router
Brand name:	HM210dp and HM210di
Product numbers:	ZAT 759 75/xxxx
Intended use:	Provide high-speed Internet access over either existing phone line or ISDN line services. For public and private use.

Linköping 2003-02-25

....

Anders Lindström
Head of Unit CPE P & S

DoC_HM210dx_ RevPA1.doc

Ericsson AB
CPE Products & Solutions

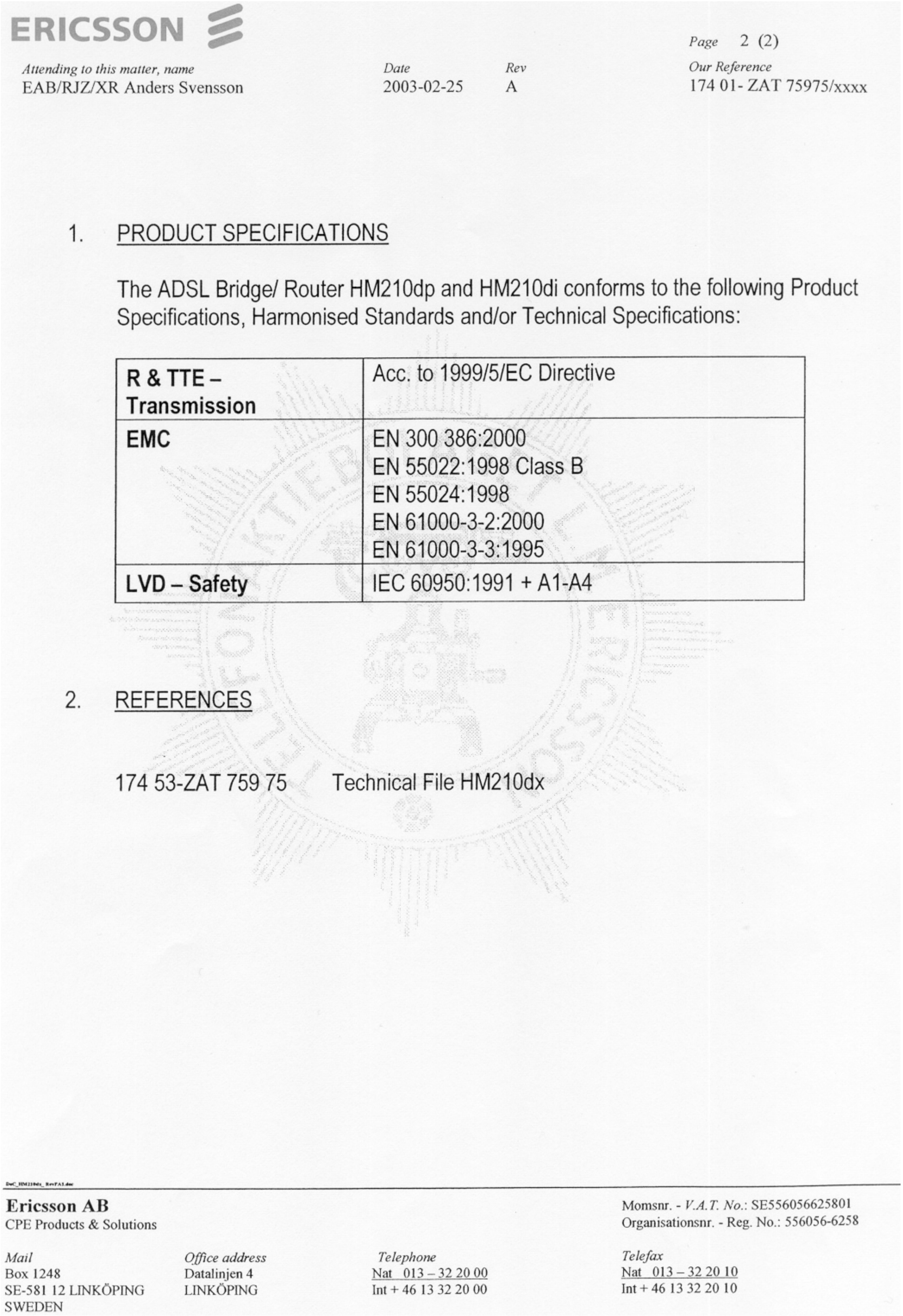
Mail
Box 1248
SE-581 12 LINKÖPING
SWEDEN

Office address
Datalinjen 4
LINKÖPING

Telephone
Nat 013 – 32 20 00
Int + 46 13 32 20 00

Momsnr. - *V.A.T. No.*: SE556056625801
Organisationsnr. - Reg. No.: 556056-6258

Telefax
Nat 013 – 32 20 10
Int + 46 13 32 20 10



ERICSSON

Page 2 (2)

Attending to this matter, name	*Date*	*Rev*	*Our Reference*
EAB/RJZ/XR Anders Svensson	2003-02-25	A	174 01- ZAT 75975/xxxx

1. PRODUCT SPECIFICATIONS

The ADSL Bridge/ Router HM210dp and HM210di conforms to the following Product Specifications, Harmonised Standards and/or Technical Specifications:

R & TTE – Transmission	Acc. to 1999/5/EC Directive
EMC	EN 300 386:2000 EN 55022:1998 Class B EN 55024:1998 EN 61000-3-2:2000 EN 61000-3-3:1995
LVD – Safety	IEC 60950:1991 + A1-A4

2. REFERENCES

174 53-ZAT 759 75 Technical File HM210dx

DoC_HM210dx_RevPA1.doc

Ericsson AB
CPE Products & Solutions

Momsnr. - *V.A.T. No.*: SE556056625801
Organisationsnr. - Reg. No.: 556056-6258

Mail	*Office address*	*Telephone*	*Telefax*
Box 1248 SE-581 12 LINKÖPING SWEDEN	Datalinjen 4 LINKÖPING	Nat 013 – 32 20 00 Int + 46 13 32 20 00	Nat 013 – 32 20 10 Int + 46 13 32 20 10

15.2.2 Safety Approvals

The HM210dp/di is approved according to the following safety standards:

- UL 1950, 3rd Ed.
- CSA C22.2 No. 60950
- IEC 60950 3rd Ed, 1999

15.2.2.1 UL 1950

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1 Do not use this product near water, for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.

2 Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

3 Do not use the telephone to report a gas leak in the vicinity of the leak.

4 Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.

CAUTION! Alway disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

15.2.3 EMC Approvals

The HM210dp/di is approved according to the following EMC standards:

- EN 300386:2000
- EN 55022:1998 Class B
- EN 55024:1998
- EN 61000-3-2:2000
- EN 61000-3-3:1995
- FCC Part 15, Class B, ANSI C63.4-1992

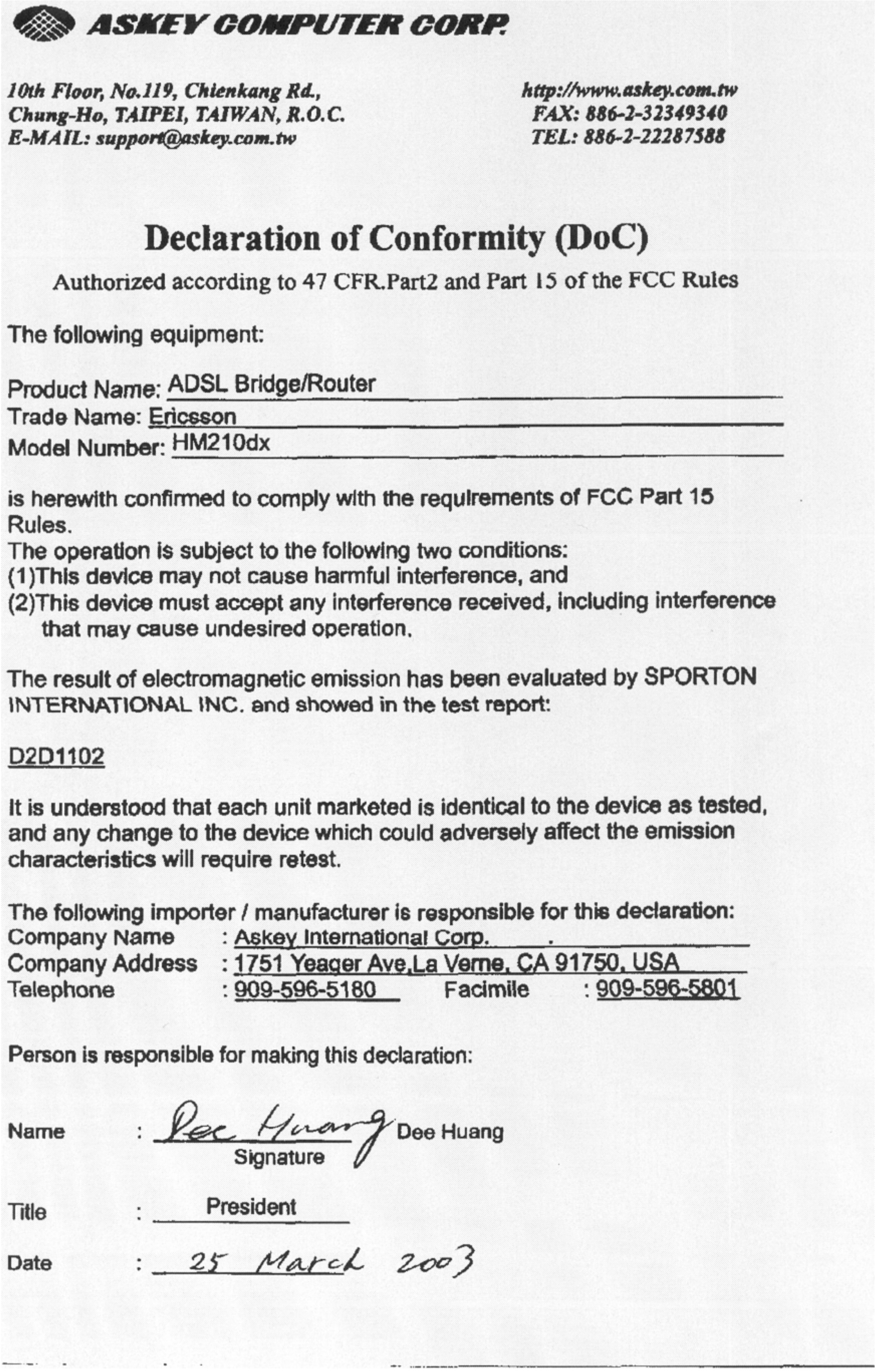
15.2.3.1 FCC Part 15

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules (Code of Federal Regulations Title 47, Telecommunications (CFR 47)). These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio or television reception. However, there is no guarantee that interference will occur in a particular installation. If this equipment does cause harmful interference to radio or television, which can be determined by turning the equipment off and on, the user is encouraged to eliminate the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna of the affected equipment.
- Increase the separation between the ADSL Modem HM210dp/di and the affected equipment.
- Connect the ADSL Modem HM210dp/di power supply to an outlet on a circuit different from that to which the affected equipment is connected.
- Consult your service provider or an experienced radio/TV technician for help.



ASKEY COMPUTER CORP.

10th Floor, No.119, Chienkang Rd.,
Chung-Ho, TAIPEI, TAIWAN, R.O.C.
E-MAIL: support@askey.com.tw

http://www.askey.com.tw
FAX: 886-2-32349340
TEL: 886-2-22287588

Declaration of Conformity (DoC)

Authorized according to 47 CFR.Part2 and Part 15 of the FCC Rules

The following equipment:

Product Name: ADSL Bridge/Router
Trade Name: Ericsson
Model Number: HM210dx

is herewith confirmed to comply with the requirements of FCC Part 15 Rules.
The operation is subject to the following two conditions:
(1)This device may not cause harmful interference, and
(2)This device must accept any interference received, including interference that may cause undesired operation.

The result of electromagnetic emission has been evaluated by SPORTON INTERNATIONAL INC. and showed in the test report:

D2D1102

It is understood that each unit marketed is identical to the device as tested, and any change to the device which could adversely affect the emission characteristics will require retest.

The following importer / manufacturer is responsible for this declaration:
Company Name : Askey International Corp. .
Company Address : 1751 Yeager Ave,La Verne, CA 91750, USA
Telephone : 909-596-5180 Facimile : 909-596-5801

Person is responsible for making this declaration:

Name : Dee Huang Dee Huang
Signature

Title : President

Date : 25 March 2003

15.2.4 Telecom Approval

The HM210dp/di is approved according to the following telecom standard:

- FCC Part 68

15.2.4.1 FCC Part 68

The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.

If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.

The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.

If the telephone company requests information on what equipment is connected to their lines, inform them of:

- The telephone number to which this unit is connected.
- The USOC jack required.
- The FCC Registration Number (indicated on the label).

The Ringer Equivalence Number (REN). Not that if several devices are connected on the same line, the RENs must not add up to more than 5.0. This REN figure is important to your telco and can be found on the equipment's FCC compliance label.

In case of operational problems, disconnect your unit by removing the modular or multi-connector plug from the telco's jack. If your regular phone still works properly, your modem has a problem and must remain disconnected and (officially) serviced or returned for repairs. If upon the above disconnection your regular phone still has problems, notify your telco that they may have a problem. If problem is still found in premises wiring not telco-installed, you are subject to a service charge. If a fault is found in telco-installed wiring, you may still be subject to a service call charge.

Unless otherwise noted in the User's Manual (e.g. fuses, etc), user may not under any circumstances (in or out of warranty) attempt any service adjustment, or repairs on this unit. It must be returned to the factory or authorizedU.S. service agency for all such work. Locations and phone number of factory or authorized U.S. service points are as following:

Company: ASKEY International Corp.

Address: 1751 Yeager Ave, La Verne, CA 91750, USA

Tel: 909-596-5180

15.2.5 Caution

Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment and invalidate approvals.

15.2.6 Power Supply

The ADSL Modem HM210dp/di is equipped with one of the following external power supply adapters:

For EU; OEM AA-161ABN, Input 230VAC/50Hz, Output - 16VAC/1A or
OEM AA-1860BN; Input 230VAC/50Hz, Output - 18VAC/600mA.

For US; OEM AA-161A; Input - 120VAC/60Hz, Output - 16VAC/1A or
OEM AA-1860; Input - 120VAC/60Hz, Output - 16VAC/600mA.

Note:

The HM210dp/di is for use only with one of the above approved supplied power adapters. In the event of equipment malfunction, replace only with an AC/DC Adapter specified by Ericsson.

15.2.7 Environmental Information

Maximum environmental values during use:

- Temperature: 0ºC to +40ºC
- Humidity: 5% to 85% RH, non-condensing.

15.2.8 Intended Use

The HM210dp/di is intended for indoor public and private use.

Glossary

ADSL

Short for *Asymmetric Digital Subscriber Line*, a technology that allows more data to be sent over existing copper telephone lines (POTS). ADSL supports data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ARP

Short for *Address Resolution Protocol*, a TCP/IP protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

ATM

Short for *Asynchronous Transfer Mode*, a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

Bridge

A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol, such as Ethernet.

Broadcast

To simultaneously send the same message to multiple recipients.

CHAP

Short for *Challenge Handshake Authentication Protocol*, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret.

Device

Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice, and modems.

DHCP

Short for *Dynamic Host Configuration Protocol*, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

DMZ

A *Demilitarized Zone* is used by a company that want to host its own Internet services without sacrificing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts.

DNS

Short for *Domain Name System (or Service)*, an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain name

A name that identifies one or more IP addresses. For example, the domain name *microsoft.com* represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages. Because the Internet is based on IP addresses, not domain names, every Web server requires a Domain Name System (DNS) server to translate domain names into IP addresses.

Downstream

The direction of a downstream signal is from the ISP/service provider to the user's computer (downloading).

DSL

Short for *Digital Subscriber Line*, which is a data communications technology that transmits information over the existing copper telephone lines (POTS). DSL takes existing voice cables that connect customer premises (CPE) to the phone company's central office (CO) and turns them into a high-speed digital link. There are many types of DSL and ADSL is one of them.

DSLAM

Short for *Digital Subscriber Line Access Multiplexer*, a mechanism at a phone company's central location that links many customer DSL connections to a single high-speed ATM line.

When the phone company receives a DSL signal, an ADSL modem with a POTS splitter detects voice calls and data. Voice calls are sent to the PSTN, and data are sent to the DSLAM, where it passes through the ATM to the Internet, then back through the DSLAM and ADSL modem before returning to the customer's PC.

Ethernet

A local-area network (LAN) architecture that uses a bus topology and supports data transfer rates of 10 Mbps. It is one of the most widely implemented LAN standards.

A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet supports data rates of 1 gigabit (1,000 megabits) per second.

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert.

Firmware

Software (programs or data) that has been written onto read-only memory (ROM). Firmware is a combination of software and hardware.

FTP

Abbreviation of *File Transfer Protocol*, the protocol used on the Internet for sending files.

Host

A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

HTTP

Short for *HyperText Transfer Protocol*, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

IANA

Short for *Internet Assigned Numbers Authority*, an organization working under the auspices of the Internet Architecture Board (IAB) that is responsible for assigning new Internet-wide IP addresses.

ICMP

Short for *Internet Control Message Protocol*, an extension to the Internet Protocol (IP). ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

IETF

Short for *Internet Engineering Task Force*, the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

IGMP

Short for *Internet Group Management Protocol*, the standard for IP multicasting in the Internet.

It's used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group.

IP address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.

Within an isolated network, you can assign IP addresses at random as long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates.

ISDN

Abbreviation of *Integrated Services Digital Network*, an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.

ISP

Short for *Internet Service Provider*, a company that provides access to the Internet.

LAN

Short for *Local Area Network*, a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings and connect workstations and personal computers. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

There are many different types of LANs Ethernets being the most common for PCs.

LED

Abbreviation of *Light Emitting Diode*, a type of control lamp on devices that indicates the status of a device.

NAT

Short for *Network Address Translation*, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

NIC

Short for *Network Interface Card*, an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

Packet

A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.

Packet switching refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

PAP

Short for *Password Authentication Protocol*, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted.

PING

A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections.

Port

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

POTS

Short for *Plain Old Telephone Service*, which refers to the standard telephone service that most homes use. The POTS network is also called the Public Switched Telephone Network (PSTN).

PPP

Short for *Point-to-Point Protocol*, a method of connecting a computer to the Internet. PPP sends the computer's TCP/IP packets to a server that puts them onto the Internet.

PPPoE

Acronym for *Point-to-Point Protocol over Ethernet*. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.

Protocol

An agreed-upon format for transmitting data between two devices. The protocol determines the following:

- the type of error checking to be used
- data compression method, if any
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message.

There are a variety of standard protocols from which programmers can choose. Each has particular advantages and disadvantages; for example, some are simpler than others, some are more reliable, and some are faster.

From a user's point of view, the only interesting aspect about protocols is that your computer or device must support the right ones if you want to communicate with other computers. The protocol can be implemented either in hardware or in software.

PVC

Short for *Permanent Virtual Circuit*, which is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or disconnected for each session.

RFC

Short for *Request for Comments*, a series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

Each RFC is designated by an RFC number. Once published, an RFC never changes. Modifications to an original RFC are assigned a new RFC number.

RIP

Short for *Routing Information Protocol*, which is a protocol that specifies how routers exchange routing table information. With RIP, routers periodically exchange entire tables.

Router

A device that connects any number of LANs. Routers use headers and a forwarding table to determine where packets go, and they use ICMP to communicate with each other and configure the best route between any two hosts. Very little filtering of data is done through routers. Routers do not care about the type of data they handle.

10BaseT

One of several adaptations of the Ethernet standard for Local Area Networks (LANs). The 10Base-T standard (also called Twisted Pair Ethernet) uses a twisted-pair cable with maximum lengths of 100 meters. Cables in the 10Base-T system connect with RJ-45 connectors.

100BaseT

A networking standard that supports data transfer rates up to 100 Mbps (100 megabits per second). 100BASE-T is based on the older Ethernet standard. Because it is 10 times faster than Ethernet, it is often referred to as Fast Ethernet.

TCP

Abbreviation of *Transmission Control Protocol*, and pronounced as separate letters. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Telnet

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

UDP

Short for *User Datagram Protocol*, a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

Upstream

The direction of an upstream signal is from the user's computer to the ISP/service provider (uploading).

VPI and VCI

A VPI (*Virtual Path Identifier*) is an 8-bit field while VCI (*Virtual Channel Identifier*) is a 16-bit field in the ATM cell header. A VPI identifies a link formed by a vritual path and a VCI identifies a channel within a vritual path. A unique and separate VPI/VCI identifier is assigned in advance to indicate which type of cells follow. Your ISP should supply you with the values.

WAN

Short for *Wide Area Network*, a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).